

Horizontal Fusion FY2004 After Action Report



**Department of Defense, Assistant Secretary of Defense for
Networks and Information Integration/DoD CIO**

05 November 2004

Revision Sheet

Release No.	Date	Revision Description
Ver 1.0	05 November 2004	FY2004 After Action Report

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
1 INTRODUCTION.....	3
2 QUANTUM LEAP-2.....	4
3 PORTFOLIO MANAGEMENT.....	8
3.1 Managing a Portfolio within the Department of Defense (DoD)	8
3.2 Horizontal Fusion Portfolio Management.....	9
3.2.1 FY2004 Objectives	10
3.2.2 Horizontal Fusion Investment.....	11
3.2.3 Horizontal Fusion Portfolio Selection Process	11
3.2.4 Funding and Accountability.....	12
3.2.5 Schedule/Integrated Master Schedule (IMS).....	12
3.2.6 Configuration Management in a Net-Centric Environment.....	13
3.2.7 Management Reviews and the Role of the Horizontal Fusion Portfolio Management Team Representative	14
3.2.8 Working Groups and Workshops	15
3.2.9 Horizontal Fusion Workspace	19
4 HORIZONTAL FUSION NET-CENTRIC OPERATIONS.....	21
4.1 Net-Centric Information Assurance (IA)	23
4.1.1 Security Policy and Procedures	24
4.1.2 Certifying and Accrediting a Services-Oriented Architecture (SOA) and Defining Discretionary Access Control-Plus (DAC+) Requirements.....	26
4.1.3 Cross-Domain Information Exchange.....	29
4.1.3.1 Technical Approach.....	29
4.1.3.2 Policy Areas.....	32
4.1.4 Secure Wireless Communications.....	33
4.1.4.1 Technical.....	33
4.1.4.2 Policy.....	33
4.1.5 Public Key Infrastructure (PKI) Certificates	34
4.1.5.1 Certificate Use Policy.....	35
4.1.5.2 Certificate Issuing Process.....	37
4.1.5.3 Technical Implementation Issues	38
4.2 Standards and Specifications.....	39
4.2.1 General	42
4.2.2 Taxonomy/Ontology.....	42
4.2.3 DoD Discovery Metadata Standard (DDMS).....	43
4.2.4 Person Data Specification	44
4.2.5 Tactical (Track) Data Standard.....	45
4.3 Development and Integration	46
4.3.1 Hardware Environment	47
4.3.2 Network Connectivity and Port/Firewall Restrictions	48
4.4 Net-Centric Enterprise Services (NCES) and Specifications.....	49
4.4.1 General	49
4.4.2 Security.....	53
4.4.3 Service Discovery	55
4.4.4 Content Discovery	57

HORIZONTAL FUSION

4.4.5	Person Discovery	58
4.4.6	Mediation Messaging/Alerts	59
4.4.7	Collaboration.....	61
4.4.8	Enterprise Service Management (ESM).....	62
5	<i>SUMMARY</i>	65
6	<i>INITIATIVE DETAILS</i>	68
7	<i>ACRONYMS</i>	75



EXECUTIVE SUMMARY

In response to Secretary of Defense Donald Rumsfeld's vision of Force Transformation, the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII)/Department's Chief Information Officer (CIO) established Horizontal Fusion in 2003 as an entity to explore and investigate new and innovative methods for sharing information and data in a Net-Centric environment. In this second year of existence, the Horizontal Fusion Portfolio has gained considerable experiences and insights into the challenges of establishing such an environment. Horizontal Fusion has established itself on the cutting edge of Net-Centric operations and warfare for the Department of Defense (DoD) specifically, and for all U.S. Government Agencies, generally. Since Net-Centricity is the important basic component of the Global Information Grid (GIG), the Horizontal Fusion Portfolio Management Team envisions that this After Action Report for 2004 will contribute to a growing body of actionable knowledge for the DoD Information Technology (IT) community and other interested parties.

The purpose of the Horizontal Fusion After Action Report is to document the results of the extensive efforts in FY2004 for the DoD. The Horizontal Fusion Portfolio, in FY2004, has made significant strides in establishing a limited Net-Centric environment on the Secret Internet Protocol Router Network (SIPRNet). The Horizontal Fusion Portfolio has 1) instituted a technical approach that can be effectively applied to accelerate integration of disparate information technologies and organizations into an interoperable network; 2) identified and published standards and specifications critical to providing a Net-Centric environment via a services-oriented architecture (SOA); 3) investigated and provided limited Discretionary Access Control (DAC) mechanisms to ensure an acceptable level of risk management for Information Assurance (IA); 4) incorporated organizations outside of DoD, including the Department of State (DoS) and the North Atlantic Treaty Organization (NATO) as a first step toward inter-agency information sharing; and 5) established the Portfolio Management paradigm as the primary management tool for these efforts.

Through the Horizontal Fusion Portal, known as the *Mars* Portal, Horizontal Fusion has demonstrated that many levels of users from edge-users to the National Command Authority will be able to task, post, process and use (TPPU) information and data in new and emerging Net-Centric methods. All members of the Portfolio have become both providers and consumers of information. Horizontal Fusion has not only proven the concept of Net-Centricity across broad guiding principles and objectives, but has also laid the foundation for an increasing sophistication and rigor that should enable the achievement of the Department's Net-Centric goals much sooner than previously anticipated.

While Horizontal Fusion is able to cite many successes in promulgating a Net-Centric environment for DoD, major challenges remain for the DoD Net-Centric community. Horizontal Fusion encountered many DoD policy barriers during the efforts this past year, particularly in the area of IA. Many of the existing DoD policies directly counter the establishment of a Net-Centric environment.



After two fiscal years of activity, Horizontal Fusion has determined that there are three general recommendations, which if implemented by the DoD, would do the most to transform our IT infrastructure into a true SOA. They are:

- All Programs of Record (POR) must begin to meta-tag their data stores to include tags for security attributes. As the SOA infrastructure matures, the POR's will then be prepared to utilize it.
- The IT security policy community must begin to review current guidelines, directives, and regulations in the context of an SOA. The current sets are inconsistent and do not support the migration toward Net-Centric operations and warfighting.
- The Department must make Public Key Infrastructure (PKI) utilization on the Secret Internet Protocol Router Network (SIPRNet) as robust as on the Non-Secure Internet Protocol Router Network (NIPRNet). Without them, strong net-centric information assurance is not achievable.

The remainder of this report provides more detailed observations and recommendations on how to transform the Department's current infrastructure and investments into an SOA to support the transformation of our warfighting forces.

The After Action Report is organized in the following manner.

- Section 1—Introduction
- Section 2—Quantum Leap-2
- Section 3—Portfolio Management
- Section 4—Horizontal Fusion Net-Centric Operations
- Section 5—Summary
- Section 6—Portfolio Initiative Details
- Section 7—Acronyms

1 INTRODUCTION

Horizontal Fusion was established by the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) in January 2003 to explore and investigate the potential feasibility of implementing an interoperable Net-Centric environment and services-oriented architecture (SOA) for the Department of Defense (DoD). The introduction of a Net-Centric environment and SOA for the Department will deliver significant improvements in battlefield operations, including near-real time access to critical information, enhanced situational awareness (both on the battlefield and globally), informed and expeditious command decision-making, and controlled and coordinated operational and tactical military movements.

In addition, Horizontal Fusion was directed to implement a new approach to information technology (IT) management within the Department—Portfolio Management. Portfolio Management marks a significant change from existing management practices, under which purchasing decisions are made on a program-by-program basis. The Portfolio Management approach, according to the “Information Technology Portfolio Management” policy directive of 22 March 2004 issued by Deputy Defense Secretary Paul Wolfowitz, will ensure that the military possesses the “right capabilities to perform its mission and conduct effective operations, eliminate outdated ways of doing business, and achieve the DoD’s Net-Centricity goals.” All DoD IT technology investments and programs will be managed as portfolios in the near future.

Horizontal Fusion has matured during the last two years and has provided the Department a “test bed” for two areas—the development of a Net-Centric environment and SOA, and Portfolio Management. Horizontal Fusion has identified and overcome many obstacles, many unforeseen during FY2003 and FY2004 in these two areas. It is the intent of this After Action Report to share the work and findings of the Portfolio with the DoD IT community and other organizations and entities interested in pursuing the establishment of a Net-Centric environment.

In FY2005, Horizontal Fusion will embark on the “operationalization” of the Net-Centric environment. Horizontal Fusion will integrate into the Collateral Space the U.S. Army XVIII Airborne Corps’ FusionNet and the DoD’s Explosive Ordinance Disposal (EOD) community’s JEODNet. This will be the first opportunity for the Department to demonstrate a Net-Centric environment in support of the warfighter during field operations.

2 QUANTUM LEAP-2

The purpose of all Quantum Leap demonstrations is to prove that an SOA is within the near-term grasp of the Department. Quantum Leap-2 emphasis areas were cross-domain information exchange, secure wireless communications, and discretionary access controls based on the roles of the individuals involved. Quantum Leap-2 was conducted on the operational SIPRNet.

For Quantum Leap-2, the following locations and organizations participated in the demonstration. All of the users accessed the Collateral Space via the *Mars* Portal on the operational SIPRNet. Some of the data providers operated from “in the field” (Ft. Benning MOUT site, Eglin AFB, and China Lake Range) at the unclassified level. Data from them was automatically populated to the Collateral Space via an SOA and software-based one-way pump. Coalition users were “simulated” at SSCC, Charleston, SC to demonstrate the cross-domain information exchange capability of the security services and role-based access. Coalition users were simulated during the demonstration to eliminate the risk of data leaks to NATO Secret-only users and to prove that the implemented security features were reliable.

The table below lists the User Sites and the Data/Application Provider Sites along with the participants.

User Sites		Data/App Provider Sites	
Washington, DC	DIA DoS MITRE OSD Pentagon	Washington, DC	DIA DoS
Adelphi, MD	ARL	Adelphi, MD	ARL
Bethesda, MD	NGA	Bethesda, MD	NGA
Ft. Belvoir, VA	INSCOM	Laurel, MD	JHU/APL
Ft Meade, MD	NSA	Monterey, CA	FNMOG
Laurel, MD	JHU/APL	Charlottesville, VA	NGIC
Hanscom AFB, MA		Norfolk, VA	JFCOM
Syracuse, NY	NY ANG	Charleston, SC	SSCC
Charlottesville, VA	NGIC	Eglin AFB, FL	JSTARS Black Hawk P-3
Norfolk, VA	JFCOM	China Lake, CA	NAVAIR
Charleston, SC	SSCC		
Ft. Benning, GA			
MacDill AFB, FL	CENTCOM		
Huntsville, AL	MSIC		
Offutt AFB, NE	STRATCOM		
Peterson AFB, CO	NORTHCOM		
Monterey, CA	FNMOG		
Oahu, HI	PACOM JICPAC		

Table 1 Quantum Leap-2 Sites

Observation and Analysis

Operational users accessed the Collateral Space through a common set of collaboration tools and services. Portfolio Initiatives implemented content management standards to ensure information posted in their specific domain could be discovered and accessed from the Collateral Space. Quantum Leap-2 provided a robust Collateral Space and network infrastructure. This eliminated the need for combat forces to manually assemble data from multiple stovepipe systems and task/coordinate through point-to-point transactions. The results included a reduced decision cycle time for a range of tactical and coalition operations.

Quantum Leap-2 contributed to transformed concepts of warfighting tactics, techniques, and procedures. It showed alternative Net-Centric options available to the commanders and troops by providing timely data fusion across disparate and geographically dispersed data sources and supported an accelerated decision-making process by utilizing sense making tools, applications, and collaboration in a web environment. This was achieved by placing intelligence, surveillance, and reconnaissance (ISR) data, command and control structures, and combat operations forces in the same virtual space. The capacity to provide access to this environment to the edge-users was also an important aspect of Quantum Leap-2.

The Portfolio demonstrated Net-Centric transformation by:

- Increasing the availability of unclassified information critical to combat decision-making on the SIPRNet utilizing the first Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG) approved software-based one-way pump and secure wireless communications
- Augmenting the collaborative command and control processes with coalition partners through the use of role-based access for strong user identification and clearance attributes in an approved cross-domain environment resulting in improved situational awareness across the coalition battle space
- Reducing the decision-making cycle time by providing access to the information sharing environment to operators up and down as well as across the chain of command
- Providing the ability to simultaneously analyze the same data by U.S. and Coalition users in disparate locations

The successful completion of the scenario used during Quantum Leap-2 showed:

- Edge-users had access to relevant, timely, disparate, metadata tagged data
- The **Mars** Portal was available when needed
- The **Mars** Portal was adaptable to suit unique edge-user requirements
- The **Mars** Portal supported operational tempo requirements

The Horizontal Fusion Portfolio implemented an SOA which provided the framework to interoperability by using the existing market-driven, standards-based information technology and by developing open architecture standards (e.g., web services, portlets, UDDI, and

HORIZONTAL FUSION

metadata tagging). Interoperability was also achieved at the system level via API standards (as defined in NCES specifications) and at the network level via *Mars* (access provided to all users regardless of the network on which they resided). Quantum Leap-2 showed edge computing power by enabling cross-domain wireless web access to the Collateral Space. Access was achieved for all echelons (field soldiers, aircraft crews, analysts, staff operators, and commanders). Both unclassified and Secret data was accessed through the *Mars* Portal on the edge-user's laptop or hand-held device.

In Quantum Leap-2, as in Quantum Leap-1, information was posted to the Collateral Space before processing. This was a continued implementation and test out of the task, post, process, and use (TPPU) concept versus task, process, exploit, and disseminate (TPED). This transformation from TPED to TPPU continues to demonstrate that all edge-users (with the proper permissions and a need-to-know adjudicated through NCES security services) can access data targeted to their specific needs, when they need it. Users could subscribe to receive alerts regarding new postings of interest to them and view them when convenient. Mission-focused COIs, standing or ad hoc, were organized around a temporary crisis and disbanded once the crisis was resolved. U.S. and Coalition users could discover appropriate ISR data provided by diverse data sources included in the Collateral Space through the application of role based, discretionary access controls. Quantum Leap-2 also proved the viability of the security core enterprise services by creating and maintaining a cross-domain, wired and wireless "trusted network" that provided an infrastructure to locate common services across the information sharing environment utilizing the *Mars* Portal.

Via *Mars*, Horizontal Fusion provided enhanced situational awareness minimizing information latency. Horizontal Fusion made available to DoD and Coalition edge-users the right information, in the right format, at the right time. Quantum Leap-2 demonstrated once again, that the DoD concept of Net-Centric capabilities and Transformation is sound and implementable. In a single search, Collateral Space users could retrieve unclassified and Secret operational and analytical data via a federation of physically dispersed data stores. Users could also access a number of browser-based "sense making" tools to mission-tailor data to meet their operational information needs.

Recommendation

Given the successes of the past two Quantum Leap demonstrations, it is now time to move the SOA baseline into an operational environment as well as into military exercises to solidify the concept of Net-Centric operations across the Department. This will reduce the scenario planning burden on the Portfolio and increase awareness of the power of an SOA to the warfighter.

3 PORTFOLIO MANAGEMENT

3.1 Managing a Portfolio within the Department of Defense (DoD)

In a policy dated 22 March 2004 entitled “Information Technology Portfolio Management”, Deputy Defense Secretary Paul Wolfowitz ordered that major changes be implemented in the managing of information technology programs within DoD. The policy requires managing all military information technology investments as portfolios, rather than on a program-by-program basis. The policy further states that “decisions on what information technology (IT) investments to make, modify, or terminate shall be based on the Global Information Grid (GIG) Integrated Architecture, mission area goals, architectures, risk tolerance levels.....and performance.” Additionally, IT portfolios “shall be managed using integrated strategic planning, integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investment strategies.”

The policy also charges the Department’s Chief Information Officer (CIO) with providing “for the Enterprise Information Environment (EIE)” which establishes a common set of capabilities that enables users to “discover, access, post, advertise, retrieve, and fuse data.” The EIE is envisioned to be the Department’s computing and communications environment and will potentially provide warfighters access to an unprecedented amount of battlespace awareness and decision support information.

The four major components of this management process, as identified by Deputy Defense Secretary Wolfowitz are below. Horizontal Fusion has embraced all four components. Each of these components of Portfolio Management, as they directly relate to Horizontal Fusion, are specifically addressed in italics.

- **Analysis**—linking mission area goals to “DoD enterprise vision, goals, objectives, priorities, capabilities” and an explanation of how those will be met and progress measured
 - *The Horizontal Fusion goals link directly to the DoD’s vision, goals, objectives, and priorities for the development of the core enterprise services within the Net-Centric Enterprise Services (NCES) Program. The Portfolio has clearly addressed a foundation of these core capabilities (i.e., Security, Services Discovery, Content Discovery, Person Discovery, and Mediation/Messaging) as well as how they were achieved and measured through the conduct of Quantum Leap-2. The selection of new members of the Portfolio was based on identified gaps and opportunities for the expansion of the services-oriented architecture (SOA) and the access controls that will lead to cross-domain information exchange. The Secret Internet Protocol Router Network (SIPRNet) security certification and accreditation in a Net-Centric environment identified risks and how these will be mitigated in a coalition environment. The Quantum Leap-2 discretionary access controlled baseline served as a proof-of-concept for net-centric Information Assurance. Finally, the transition of the Collateral*

HORIZONTAL FUSION

Space, which is a loosely coupled distributed network of services, to the operational forces will help determine the strategic direction for Net-Centric activities and processes in FY2006.

- **Selection**—identifying the best mix of IT investments to achieve goals and transition to future architectures
 - ❑ *The Portfolio's identification of the best fit, balance, and impact of IT Portfolio Initiatives to achieve Net-Centric goals and plans has been well coordinated with the strategic guidance provided by the United States Joint Forces Command (USJFCOM/J9) that includes the services, the Combatant Commands (COCOMS), the Joint Chiefs of Staff (JCS), and the intelligence agencies, as well as a roadmap for an accelerated delivery of the SOA to operational forces.*
- **Control mechanisms**—ensuring individual programs “are managed in accordance with cost, schedule, performance and risk baselines, and documented technical criteria” as well as the Department’s GIG Integrated Architecture
 - ❑ *The Portfolio ensured that individual Portfolio Initiatives were managed in accordance with cost, schedule, performance and risk baselines, and documented technical criteria. The traditional budget process and project development guidelines of DoD have proven a challenge to the Portfolio model of IT acquisition and have resulted in a set of recommendations from the Horizontal Fusion Portfolio Manager to modify the process.*
- **Evaluation**—systematically assessing and measuring actual contributions of the Portfolio and support adjustments to the mix of Portfolio projects
 - ❑ *Both Quantum Leap-1 and Quantum Leap-2 have been effective in providing the DoD CIO an operational tempo that systematically measures actual contributions of the Portfolio's SOA. The capacity to enable a cost effective framework to the interoperability of existing programs of record has been a substantial leap forward in the Department's quest for Net-Centric operations and warfighting. These Net-Centric enterprise demonstrations have included several DoD/U.S. Government components and have supported adjustments to the mix of Portfolio projects, as necessary.*

3.2 Horizontal Fusion Portfolio Management

Since Portfolio Management is a relatively new management concept for the Department, few directives exist for establishing an effective structure. The basis for the Horizontal Fusion Portfolio Management conduct is Deputy Defense Secretary Wolfowitz's policy directive on Portfolio Management. This directive has served as the basis for the Horizontal Fusion Portfolio Management practices; yet, much needs to be learned and implemented as the Department moves towards full inclusion of Portfolio Management. In this section, observations/analyses and recommendations to improve the process have been captured.



There were many internal challenges associated with managing the Horizontal Fusion Portfolio including establishing Work Breakdown Structures (WBS); moving funding from the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) to different DoD or U.S. Government organizations; establishing contracts and procuring hardware; hiring personnel and educating them on the goals of Horizontal Fusion; and ensuring that each Portfolio Initiative could comply with an aggressive development schedule. To alleviate these challenges, the Portfolio Manager and the Horizontal Fusion Portfolio Management Team developed a management strategy and implemented management tools designed to not only allow each Initiative to succeed in becoming web-enabled and an active participant in the SOA, but more importantly, work together as a team to solve the problems in developing an SOA and achieving Net-Centric operations. The sections below cover the management strategy and the tools used to manage the Portfolio during FY2004.

Because of strong ASD/NII sponsorship and the incorporation of the Portfolio Management paradigm, Horizontal Fusion approached issues with a “can do” attitude, while the Portfolio Manager provided the overhead necessary to facilitate participation in this inter-service and interagency community of interest (COI). Since Horizontal Fusion approached issues from an enterprise perspective, and not from a proprietary perspective, the Portfolio exhibited a bias for action that did not exist elsewhere.

3.2.1 FY2004 Objectives

In FY2004, the Horizontal Fusion Portfolio continued to expand and improve upon the Net-Centric warfare capabilities developed during FY2003. Horizontal Fusion implemented an SOA, several elements of the Defense Information Systems Agency’s (DISA’s) core enterprise services, and took the first steps towards establishing a SIPRNet role-based access environment. Specific focus areas for FY2004 were cross-domain information exchange, secure wireless communications, and transitioning to operations the FY2004 version of the Collateral Space. The Portfolio Initiatives that made up Horizontal Fusion focused on web-enabled data, web services, and browser-based “sense-making” tools in support of Net-Centric warfare. The cross-domain information exchange objectives and the implementation of Discretionary/Mandatory Access controls will become the foundation for the U.S.-Coalition partners’ near real-time information sharing and is consistent with the Information Assurance Task Force plan for net-centric Information Assurance.

The integration and interoperability of the Initiatives, intended to improve speed-of-command, decision support, and transformational warfare in a Net-Centric environment, was successfully demonstrated during Quantum Leap-2.

3.2.2 Horizontal Fusion Investment

The FY2004 Portfolio was composed mostly of individual Programs of Record, representing the major services and several government agencies. These individual Initiatives provided the services, data, and tools that demonstrated the concepts of cross-domain information exchange, secure wireless, core services, sense-making, transformation, data sharing via Federated Search, and data publication in the Collateral Space. Each of these Portfolio Initiatives worked together as a team to improve the decision support, knowledge sharing, and information sense-making capabilities to the COIs spanning across the intelligence and operations areas. For a detailed listing of the Initiatives and their contributions, please refer to Section 6, Portfolio Initiative Details.

3.2.3 Horizontal Fusion Portfolio Selection Process

Observation and Analysis

The primary goal of the Portfolio selection process was to ensure that a selected Portfolio Initiative's program or project could potentially advance the realization of Net-Centricity, improve decision support capabilities, align with user objectives and GIG implementation priorities, and extend to an operational Net-Centric environment relatively quickly. The Horizontal Fusion Portfolio Management Team followed a structured approach in the selection of Portfolio Initiatives for FY2004. The Portfolio Manager invited interested organizations within DoD and other departments to participate in a Portfolio Candidates' Workshop in July 2003. Organizations then submitted Statements of Work (SOWs) for proposed Portfolio Initiatives within three weeks of the conclusion of the workshop. The Engineering Review Board (ERB), composed of Horizontal Fusion Portfolio Management Team members, evaluated these SOW submissions on the basis of three broadly defined selection criteria—fit, balance, and impact—each of which were further divided into five to six sub-criteria. The ERB used a scorecard tool to assist in the evaluation of each SOW in regard to these criteria, then compiled individual scorecards into a consolidated scorecard to provide a quantitative justification for its staff recommendation of Portfolio composition to the Portfolio Manager. With this staff recommendation and quantitative support, the Portfolio Manager selected the FY2004 Horizontal Fusion Portfolio in concert with the DoD CIO. The Portfolio Manager announced the FY2004 Horizontal Fusion Portfolio in early October 2003.

In FY2004, the announcement of the FY2005 Portfolio Selection Process was disseminated in two venues, 1) the Horizontal Fusion public website and 2) a United States message text format (USMTF) cable to all Services, Agencies, and COCOMs. A one-day Portfolio Candidates' Conference was also held, in addition to the Net-Centric Boot Camp, to further educate and enlighten the potential Net-Centric operations community to the benefits of participation within Horizontal Fusion.

Recommendation

The basic approach of the Portfolio selection process was sound.

3.2.4 Funding and Accountability

Observation and Analysis

The Portfolio Manager earmarked funding for each Portfolio Initiative based upon their SOW and Rough Order of Magnitude (ROM) submissions. At the FY2004 Kickoff Workshop in October 2003, the Portfolio Manager provided each Portfolio Initiative the opportunity to refine its SOW, with supporting WBS, in preparation for negotiations. Funding allotments were then made on a Firm Fixed Price (FFP) basis in November 2003. The Portfolio Manager then initiated the Military Interdepartmental Purchase Request (MIPR) process to fund the sponsoring organization of each Portfolio Initiative. Receipt of funding to Portfolio Initiatives ranged from December 2003 to March 2004. Portfolio Initiatives were held accountable for funding expenditures during the two Quarterly Reviews with the Portfolio Manager, as well as through continuous coordination between the Portfolio Initiative Program Manager and the Portfolio Initiative's Horizontal Fusion Portfolio Management Team Representative. Financial information from each Portfolio Initiative was consolidated for the Portfolio Manager.

A three to six month funding delay provided a significant management challenge to the Portfolio Initiatives. It delayed start-up for new Portfolio Initiatives, and it interrupted continuity for existing Portfolio Initiatives—those that participated in FY2003. As there was no schedule relief (see Schedule/Integrated Master Schedule (IMS) discussion below), many Portfolio Initiatives found themselves in the position of expending nine months of planned effort over a five-month period. Other Portfolio Initiatives were able to overcome this delay in funding by either working at risk or by borrowing developers and/or other support from existing contract vehicles within their organizations through Special Project Authorizations or other similar government/industry common practices. Finally, one contractor organization was unable to overcome the delay in funding and was subsequently left the Horizontal Fusion Portfolio in 2004.

Recommendation

The existing DoD funding apparatus lessens the impact of Portfolio Management. A funding apparatus needs to be established within DoD to accommodate the flexibility required by the Portfolio Management approach.

3.2.5 Schedule/Integrated Master Schedule (IMS)

The high-level milestones for the Horizontal Fusion Portfolio were announced at the October 2003 Kickoff Enterprise Integration Workshop (EIW). The IMS attempted to carry forward key tasks from individual Portfolio Initiative project plans into the tasks of the Portfolio as a whole, creating “hooks” into the IMS. The focus of the IMS was schedule management,

primarily from an enterprise perspective. Horizontal Fusion did not manage the developmental schedule and activities for each individual Portfolio Initiative.

Many Portfolio Initiatives adopted a spiral model of development in order to keep pace with the momentum of the Portfolio and planned development activity. The announced date of August 11th for Quantum Leap-2 served as a “stake in the ground.” Two key milestones were defined leading up to that date 1) the deadline for submission of a Portfolio Initiative’s Systems Security Authorization Agreement (SSAA) and 2) the Code Freeze date for the development of software functionality.

Some Portfolio Initiatives indicated a desire for establishing additional code freeze dates—with thin slices of functionality to be delivered at interim points—in order to mitigate the huge push of development activity as the Code Freeze date approached.

In spite of funding delays and schedule rigidity, the Portfolio, collectively, and the Portfolio Initiatives, individually, performed high quality work in pursuit of the goals and objectives of Horizontal Fusion for FY2004. The Horizontal Fusion Portfolio, by virtue of its fixed schedule, its FFP cost structure, and its collaborative and collective problem-solving environment, set a course of demonstrating the concept of Net-Centricity.

Recommendation

Direct more DoD programs to adopt the Portfolio Management paradigm. The Portfolio Management approach provided the needed flexibility to accomplish objectives in a quicker, cheaper, and more responsive manner than traditional IT acquisition management practices.

3.2.6 Configuration Management in a Net-Centric Environment

The objective of Configuration Management within a Net-Centric environment is to accommodate change, optimize the reuse of standards and best practices, ensure that all requirements remain clear, concise, and valid, and communicate changes to users that are prompt and precise. To effectively execute configuration management within a Net-Centric environment, it must be inherently flexible and agile in order to enable large teams to work together in a stable and controlled environment.

Observation and Analysis

Horizontal Fusion is an agile integration environment and it is difficult to dictate configuration management processes and procedures to programs of record that operate in a traditional program management environment. All Portfolio Initiatives need to follow a defined and structured configuration management plan as required in a Net-Centric environment and the time and effort has to be dedicated to develop an all encompassing configuration management plan. The processes should be streamlined and flexible to allow for time constraints so developers cannot avoid the steps necessary within a mixed environment, which also alleviates the risk introduced when processes are not followed. A major part of the overarching configuration management plan would be to ensure that all participants have a configuration



management process established to internally manage individual Portfolio Initiatives. Working in concert, both the Portfolio Initiatives and the Horizontal Fusion Portfolio Management Team must identify as configuration controlled items the relevant specifications, design documents, and code to include version identification, delta identifiers, and derivation records to produce the enterprise Net-Centric configuration management plan.

Configuration management has an impact on the overall security of any Net-Centric environment. Configuration management provides the identifiable configuration items used by integrators, as well as security for certification and accreditation (C&A). Therefore, security is an integral part of the configuration management process. Security configuration management needs to publish standards that detail an agile and flexible security process with established thresholds for security scans. Definition of success criteria and boundaries of an SOA that identifies changes affecting security are required, so a complete audit does not have to be done unless it affects security. As security continues to evolve and as governments and other regulatory bodies pass legislation concerning security, tighter configuration management control policies and processes will need to be levied against systems.

Recommendations

Tailor configuration management processes to be flexible in a SOA environment.

The Portfolio configuration management requires automated problem tracking and configuration management tools to help maintain accurate records of proposed changes, ownership, test results, and implemented changes.

A Portfolio configuration manager is required to provide guidance and control.

3.2.7 Management Reviews and the Role of the Horizontal Fusion Portfolio Management Team Representative

Observation and Analysis

The Portfolio Manager effectively facilitated two-way communications within the Portfolio. The Portfolio Manager conducted Quarterly Reviews on a staggered schedule at each of the EIWs. The Quarterly Reviews consisted of 30-minute sessions for review of each Portfolio Initiative's status with respect to the planning documents (SOW, WBS, cost estimate, and schedule), and an active dialog between the Portfolio Initiative Program Manager and the Portfolio Manager. Artifacts for each Quarterly Review consisted of a Quarterly Review Status Chart (Quad Chart), Horizontal Fusion Initiative Control Chart, and Horizontal Fusion Initiative Control Point Identification Chart. While the Control Chart identified risks and management activities thereof, the Control Point Identification Chart tied cost and schedule performance back to its identified WBS tasks. The Portfolio held spotlight reviews from March 2004 to May 2004 as the Code Freeze date approached. The Horizontal Fusion Portfolio Management Team Representatives rated each of their Portfolio Initiatives as *red*, *yellow*, or *green* in each of five categories, to facilitate their timely accomplishment of stated objectives. The Horizontal Fusion Portfolio Management Team updated spotlight ratings for

the Portfolio Manager on a weekly basis, and the Portfolio Initiative Program Managers themselves held the spotlight reviews with the Portfolio Manager at the April 2004 EIW.

In addition, each Portfolio Initiative was assigned a Horizontal Fusion Portfolio Management Team Representative. The Representatives were responsible for ensuring that the Portfolio Initiative had a WBS, was meeting the schedule milestones, and was following the budget outlined in the WBS. These Horizontal Fusion Portfolio Management Team Representatives were very effective in minimizing the risk associated with each Portfolio Initiative. But a far more crucial role played by the Horizontal Fusion Portfolio Management Team Representative was ensuring that each Portfolio Initiative was contributing to the greater good of the Portfolio. These Representatives could devote one-on-one time in making sure the Portfolio Initiatives understood the goals of Horizontal Fusion—that Horizontal Fusion was not about individual achievement, but about achieving a greater capability for DoD.

Recommendation

The combination of the Horizontal Fusion Portfolio Management Team Representatives and direct one-on-one sessions with the Portfolio Manager was a most effective way of ensuring that Portfolio Initiatives met their individual goals and, more importantly, were focused on helping the Portfolio achieve its goals and objectives.

3.2.8 Working Groups and Workshops

Observation and Analysis

The Portfolio held EIWs on a monthly basis from December 2003 to June 2004, and then in September 2004, alternating locations between the National Capital Region and Charleston, South Carolina. Each EIW began on Tuesday morning and concluded late Thursday afternoon/evening, with Fridays available for Portfolio Initiative Quarterly Review sessions and a “power wash” by the Horizontal Fusion Portfolio Management Team. The agenda, published the week prior to the EIW, was front-loaded with Portfolio-wide issues on Day One, and a concentration on Working Group activities scheduled on Days Two and Three.

The Portfolio formed two major Working Groups within the Portfolio 1) the Integration Working Group (IWG) which had two Sub-Working Groups, Data Management and Web Components and 2) the Security Policy Working Group (SPWG), which also had two Sub-Working Groups, Cross-Domain Information Exchange and Secure Wireless. All working groups and sub-working groups were managed by purpose, objectives, and tasks. Meeting agendas were clearly defined and announced (see Table 1 below for the details of each Working Group and Sub-Working Group). Sub-working groups also formed focus groups to address particular issues/problems necessary to accomplish the tasks and objectives that required more detail. The Horizontal Fusion Portfolio Management Team captured key tasks within the IMS and tracked them accordingly. Upon completion of its key tasks, each working group stood down. Working Group sessions were held during each EIW and also in the interim between EIWs. These interim sessions were scheduled and de-conflicted from other Portfolio activities through the use of a centralized calendar that set recurring daytime

HORIZONTAL FUSION

combinations for meetings on a bi-weekly basis. Meeting times were set to accommodate Portfolio Initiative participation from United States Pacific Command (USPACOM) in Hawaii to the North Atlantic Treaty Organization (NATO) in Europe. After the Code Freeze date, all working groups stood down with the exception of the IWG. At this point, IWG meetings were held on an as-needed basis, and the Chief Engineer held a daily ERB teleconference (by invitation only) and a daily Developers' Call (open to all and immediately following the ERB).

WORKING GROUP/SUB-WORKING GROUP	PURPOSE	OBJECTIVES	TASKS AND AGENDA
Integration	To standardize processes for Portfolio Initiatives to integrate into the <i>Mars</i> Portal	<ul style="list-style-type: none"> • Review and refine existing standards for the <i>Mars</i> Portal • Support public key infrastructure (PKI) and user roles and profiles • Develop new, refine existing, and implement processes (configuration management, security, test, etc.) to all Portfolio Initiatives to integrate data and web components into the <i>Mars</i> portal 	<ul style="list-style-type: none"> • Maintain the Quantum Leap-1 Standards and Guidance Document dated 16 May 2003 • Coordinate with Data Management, Web Components, and Security Policy Working Groups
Data Management	To develop/refine Collateral Space data standards	<ul style="list-style-type: none"> • Develop, refine, and implement data standards to support discovery, alerts, collaboration, messaging, and posting data to the Collateral Space • Register data standards and taxonomies within the appropriate COI of the DoD Extensible Markup Language (XML) Registry 	<ul style="list-style-type: none"> • Work closely with DoD CIO Net-Centric Data Management Strategy Group to implement strategy for Horizontal Fusion Portfolio and provide feedback <ul style="list-style-type: none"> ▪ Review DoD Net-Centric Data Management Strategy dated 9 May 2003 ▪ Review other data management strategy and standards documents • Separate Data Management Standards from Web Services Standards • Recommend changes to Quantum Leap-1 Standards and Guidance Document dated 16 May 2003 • Coordinate with Integration and Web Components Working Groups
Web Components	To develop/refine Collateral Space access and data exploitation standards	<ul style="list-style-type: none"> • Develop, refine and implement web services for discovery, alerts, collaboration, 	<ul style="list-style-type: none"> • Separate Data Management Standards from Web Services Standards • Recommend changes to Quantum Leap-1 Standards and Guidance

HORIZONTAL FUSION

WORKING GROUP/SUB-WORKING GROUP	PURPOSE	OBJECTIVES	TASKS AND AGENDA
		<ul style="list-style-type: none"> messaging, and posting data to the Collateral Space Register Web Services 	<p>Document dated 16 May 2003</p> <ul style="list-style-type: none"> Coordinate with Integration and Data Management Working Groups
Security Policy	To review, interpret, and provide recommendations to support Net-Centric operations	<ul style="list-style-type: none"> Approval, publication, and dissemination of required changes to existing DoD Security/Information Assurance (IA) policies to allow cross-domain information exchange Approval, publication, and dissemination of a DoD-level security accreditation policy of operating in a Net-Centric environment 	<ul style="list-style-type: none"> Investigate policy issues related to Smart Software Agents, PKI, processes for C&A, and technical capabilities Develop changes to DoD Security/IA policies to allow cross-domain information exchange Develop proposed DoD-level security accreditation policy for operating in a Net-Centric environment Coordinate with Cross-Domain Information Exchange and Secure Wireless Working Groups
Cross-Domain Information Exchange	Share information in the Collateral Space across multiple coalition and classified networks	<ul style="list-style-type: none"> Remove roadblocks to implementation Recommend changes to DoD Security/IA policy where necessary with respect to Cross-Domain Information Exchange 	<ul style="list-style-type: none"> Identify roadblocks Review DoD and related communities Security/IA policies Assess multiple PKI implementations Investigate similar and current Portfolio Initiatives for Cross-Domain Information Exchange Advise Portfolio Initiatives on potential solutions Coordinate closely with Security Policy and Secure Wireless Working Groups
Secure Wireless	Identify and assess current and emerging commercial and government secure wireless communications capabilities and evaluate their use to support transformational warfare	<ul style="list-style-type: none"> Identify optimal (cost, schedule, security, etc.) secure wireless communications capabilities Develop strategies and approaches for their implementation Identify any and all roadblocks to implementation Review existing DoD IA policy with 	<ul style="list-style-type: none"> Determine DoD wireless and tactical radio Portfolio Initiatives that may have a bearing on the program Liaison to and assist the DoD Joint Tactical Radio System (JTRS) Program Office and ASD/NII wireless directorate Determine wireless communications bandwidth needs and capacity limitations Identify entry points to the Horizontal Fusion Collateral Space

HORIZONTAL FUSION

WORKING GROUP/SUB-WORKING GROUP	PURPOSE	OBJECTIVES	TASKS AND AGENDA
		respect to secure wireless communications and develop necessary changes and recommendations	<ul style="list-style-type: none"> • Create documentation to reflect work and support recommendations • Plan and deliver secure wireless capability to support Quantum Leap-2 • Assess additional IA needs for Quantum Leap-2 to ensure holistic protection of information/infrastructure • Coordinate closely with Security Policy and Cross-Domain Information Exchange Working Groups

Table 2 Horizontal Fusion Working Groups and Sub-Working Groups

Working Groups were the primary means of tracking the progress of Portfolio Initiatives and effective in tackling problems that affected the entire Portfolio. The Working Groups were also an effective means of communicating the direction and needs of the Portfolio as requirements and focus was refined.

Often described by some Portfolio Initiatives as “necessary evils,” since they took time away from development activities, EIWs provided valuable information and collaboration that could have never been accomplished through the context of Working Group meetings held through teleconferences. Some Portfolio Initiatives indicated that less frequent workshops, at six-week intervals, would allow more time for development in the interim. Portfolio Initiatives expressed the desire for the Horizontal Fusion Portfolio Management Team to issue the agenda earlier, therefore enabling the Portfolio Initiative Program Managers to ensure that the right people attend each EIW. Also, as some presentations and/or working group sessions might have had a wider audience than those in attendance, a teleconference or on-line meeting capability would be beneficial to allow those not present to “virtually” attend the meeting. The Portfolio noted the delicate balance between offering highly effective collaborative tools, those that encourage folks to stay home, and the face-to-face collaboration that occurs during the EIWs, which cannot be replicated virtually. Another need identified was to hold a “technical” workshop sometime during the year to work out solely technical, development issues not appropriate for the normally wide audience that attends the monthly EIW. Finally, provisioning a local area network (LAN) at the EIWs would facilitate information exchange within the Portfolio amongst all attendees, as well as with those developers at their home station.

Recommendations

Agendas for the EIWs need to be published as early as possible to allow the Portfolio Initiatives to send the right people to participate in the scheduled sessions. In addition, other



collaboration techniques (telephone-conference, net meeting, etc.) need to be investigated/implemented to allow participation from personnel that cannot attend but would greatly benefit from key presentations.

3.2.9 Horizontal Fusion Workspace

Observation and Analysis

Horizontal Fusion maintained a collaborative workspace on the Non-Secure Internet Protocol Router Network (NIPRNet) to support the communications built around these activities: The Horizontal Fusion Workspace is a collection of individual workspaces on the NIPRNet, one per Working/Sub-working Group, and a high-level workspace for the Horizontal Fusion Portfolio Management Team items (including the master calendar), tied together through Uniform Resource Locator (URL) links into a single, virtual Horizontal Fusion Workspace. Based on Microsoft SharePoint, the Horizontal Fusion Workspace provided a low-cost, Secure Socket Layer (SSL) access to its collection of tools and information to support the communications needs of the Portfolio and its temporally and geographically dispersed Portfolio Initiatives. The Horizontal Fusion webmaster controlled both access to and authorizations on the Horizontal Fusion Workspace. Workspace utilities included document libraries for file management, lists for news and new document announcements, lists for action items, contact information, discussion boards for asynchronous communication on specific topics, and a calendar that listed events, to include EIWs, Working Group meetings, and high-level milestones. The Horizontal Fusion Workspace also allowed users to subscribe to lists and libraries for email notification updates to workspace content.

While the structure of the Horizontal Fusion Workspace had improved over the single workspace used during FY2003, it was noted that many of the personnel were unable to locate information on the workspace. Portfolio Initiatives also noted that use of the discussion threads within discussion boards was not effective. Other limitations of the Horizontal Fusion Workspace were the lack of chat capability, no collaborative tool capability (Groove, SameTime, NetMeeting, etc.), and no application sharing within the Horizontal Fusion Workspace. Many Portfolio participants used AOL Instant Messenger (AIM) for chat/instant messaging capability. Finally, one Portfolio Initiative indicated a desire to have a SIPRNet instantiation of the Horizontal Fusion Workspace that was as similar as possible to the NIPRNet instantiation, as the work environment for that Portfolio Initiative precluded ubiquitous NIPRNet access, thereby limiting its access to Horizontal Fusion Workspace tools and content.

Recommendation

An optimum solution for the Horizontal Fusion Workspace would be to provide a virtual space where software applications, documents, and people are directly accessible—chat and audio/video conferencing (privately, when required) included. Within chat, both text and URLs should be included. Any document servers should be federated and provide shared whiteboard (with ability to save), URLs, documents and spreadsheets, and document



editing/change tracking. An ability to search for people and data on the Horizontal Fusion Workspace is also a necessity.

4 HORIZONTAL FUSION NET-CENTRIC OPERATIONS

To achieve Net-Centric operations, Horizontal Fusion has focused on the creation and growth of a Services-Oriented Architecture (SOA). This section will provide an overview of this SOA and define its place within Horizontal Fusion. Before examining the details behind Horizontal Fusion's implementation of the SOA, a brief description of an SOA is provided.

An SOA is a collection of discoverable applications (called "services") distributed throughout a network/network of networks/enterprise. The concept of an SOA is not new. However, with the advent of the World-Wide Web (WWW) and the development of infrastructure protocols and services (e.g., Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Universal Description, Discovery and Integration (UDDI), etc.), implementation of a largely distributed SOA has become possible.

Some services are considered "core" services, which means they provide key infrastructure capabilities to the enterprise. Others provide data, specific community of interest (COI) services (i.e., weather) or provide sense-making capabilities (i.e., data visualization on a map). Services operate in either a "request/response" or "publish/subscribe" mode. Some services send data or application content only upon a request from another service or user. Others provide an ability to subscribe to content and the infrastructure service then subsequently provides data that the user has requested when it is available.

In the SOA, all services, singly or in concert with each other, provide capabilities and/or data, regardless of location and independent of communication paths. This is comparable to making a phone call. You pick up the phone (regardless of its manufacture), make the call, and connect to the appropriate person—without knowing the different phone switches and pathways required to complete the call. It does not matter that the signal may be transferred from copper wire to fiber to satellite. The call is completed and data is exchanged.

From a security perspective, an attribute-based access model protects the SOA. That is to say, users with certain attributes (e.g., clearance, role, nationality) will only be able to access certain data or services based on established releasability rules. All of this is performed by a union of core security services, security metadata tags, user attributes, releasability policy and adjudication. The data is labeled by type of data it is (called "metadata tagging") and by security classification.

A service registry manages information about services (location of providers, implementations, and their metadata). These services can easily be discovered (like the yellow pages part of a phone book). There is also a user registry, which manages information about the users in the enterprise (name, encrypted login passcode, role, and clearance). These users can be easily discovered (like the white pages of a phone book).

The SOA is the framework that allows legacy programs to become interoperable and Net-Centric. Programs that currently support one set of users via dedicated communication paths



on stand-alone hardware platforms can now support any DoD user, without regard for user connectivity and/or hardware platform. The SOA core services provide the interface between the user and the legacy program. The security services ensure that the user can trust the program and vice versa. The registries allow the user to find the program that it needs (without having to know that the program even exists) and to find other users that share common interests. Legacy programs no longer need to worry about point-to-point interfaces with other programs. Just as the user is able to discover the required programs via registries, programs can discover other programs and become interoperable by utilizing the same core services.

These legacy programs connect to the SOA framework by following standards and specifications. As the names imply, standards and specifications are common ways of developing programs. The program itself can offer unique data or services, but they make that data available to the user in a common way. Some of these standards and specifications are used throughout the commercial world to develop the internet and the World Wide Web. These commercial standards allow different computers (Mac v. PC) using different operating systems, different versions of software, and different web browsers to access the same web page and perform the same functions. Some standards and specifications are unique to the government. The level of security required to operate on the DoD networks is much more robust than on the internet, therefore security standards and specifications are developed specifically to address government requirements.

Service Oriented Architectures (SOAs) provide an interoperable framework for sharing data and knowledge dissemination. In order to share data, there must be a common understanding of the data semantics. Ontology's and taxonomies provide the means of categorizing and managing the vast amounts of data to be shared. Many Communities of Interest (COI) categorize their data into a taxonomy; a hierarchical model of concepts. For example, the weather COI can categorize the type of data it works with (i.e., temperatures, wind speed, cloud cover, etc.). Horizontal Fusion mapped several different COI taxonomies into a single taxonomy so that users of the SOA understand concepts across COIs. This provided a common frame of reference in which to register data sources at a high level for the federated search service. The ontology takes the taxonomy further by capturing relationships between concepts. This allowed the query engine to expand queries to concepts related to those expressed in the original queries. For example, a taxonomy used to categorize Red Force Weapon Systems would include Surface-to-Air Missiles and Anti-Aircraft Systems. The ontology would establish a relationship between these two concepts (a Surface-to-Air Missile can also be considered an Anti-Aircraft System). When a user searches for information concerning a certain type of Surface-to-Air Missile, the query system would not only search data sources that have registered as having data about Surface-to-Air Missiles, but also search data sources that have registered as having data about Anti-Aircraft Systems.

The primary user point of entry is through the *Mars* Portal. A portal is a web page that allows the user to get to any number of services or capabilities from just one site – like AOL or MSN. Users accessing the portal present their public key infrastructure (PKI) certificate for authentication. Once access to the portal is approved, access to any of the capabilities that are part of the portal is granted (single sign-on). The security services, clearance policy decision services, and security adjudication services are responsible for the overall security of the SOA



and are used by both core and non-core components to perform security policy decisions based on role, clearance, clearance dominance, and nationality. Services are entered into the registry via the Net-Centric Enterprise Services (NCES) Service Discovery Service (SDS). Once registered, services are readily discoverable through a standard UDDI directory. Content Discovery provides a federated search across multiple databases. The Registration Web Service (RWS) is used by data and content providers to register their services into the Content Discovery capability. Messaging provides the publish/subscribe mechanism used by the enterprise (e.g., Alerting). The Global Directory Service (GDS) is the core user directory infrastructure (used to authenticate users and services), which is extended by the Person Discovery Service to provide additional “Find the Expert” capabilities. The specifications of the *Mars* Portal itself included the Java Specification Request Number 168 (JSR-168) portlet specification and the PortalRbacBean (which is the Horizontal Fusion identity assertion service) specification that the portlet developers used to integrate into GDS. Each core component had an accompanying specification that governed how to consume the service properly. The core components of the Horizontal Fusion architecture are identified in Figure 1.



Figure 1 Horizontal Fusion Core Components

4.1 Net-Centric Information Assurance (IA)



Security must be designed into networks and systems from the beginning and implementation of an SOA is no exception. Information assurance and interoperability, critical elements of "net-readiness," must be the rule rather than the exception. This is the benefit of Horizontal Fusion's contribution to Net-Centric IA. As the Department of Defense (DoD) migrates to a Net-Centric environment, SOA must ensure secure, seamless exchange of information and implement safeguards to defend and protect against unauthorized external/internal access to its Net-Centric functional capabilities, NCES infrastructure, and Service/Agency/joint-provided data sources. Net-Centric IA must support information exchange across multiple security domains between joint commands, intelligence communities, the Department of Homeland Security (DHS), DoD Agencies, and multinational components while defending against attacks from the low side and preventing leakage of data from high-to-low domains.

In FY2004 Horizontal Fusion developed an IA architecture that protected the shared data sources by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. IA involved assessment of operational risk and assurance that Director of Central Intelligence Directive (DCID) 6/3 certification and accreditation requirements are met through informed Designated Approving Authority (DAA) risk acceptance and approval. For this enterprise environment, the DoD Chief Information Officer (CIO) had designated a single DAA for the Horizontal Fusion Portfolio.

4.1.1 Security Policy and Procedures

One of the key goals of Horizontal Fusion was to demonstrate secure communications (wireless or otherwise) and cross-domain information exchange from within a SOA. To achieve these goals, Horizontal Fusion targeted to deliver an SOA that met Protection Level (PL)-5 requirements following DCID 6/3 guidelines. DCID 6/3 and security policies in general were not developed to support an SOA and, therefore, were in conflict with objectives of an SOA (trusted operating systems vs. security services architecture). The Horizontal Fusion Portfolio did manage to achieve DCID 6/3 PL-3 requirements by moving beyond Discretionary Access Control (DAC) towards Mandatory Access Control (MAC) requirements. The Portfolio labeled this effort as Discretionary Access Control-Plus (DAC+), where the plus represented those aspects of MAC that were implemented. In summary, the attributes of DAC+ included the following:

1. All personnel, servers, and mobile code signers were issued a PKI certificate as a key component of the architecture. The certificates were used by the infrastructure (portal, back-end services, etc.) as the identity token to provide client and server authentication when accessing resources, as well as the digital signature and encryption for SOAP messages, Security Assertion Markup Language (SAML) assertions, labeling of data, and whatever mobile components traverse the enterprise.
2. All data in the enterprise, whether in motion or at rest, was labeled with a metadata tag which indicated classification of data. Labeling in this sense refers to the binding of the clearance information to the data elements in such a manner that it cannot be illegitimately changed or severed.
3. Back-end services performed auditing of a defined set of events (e.g., service access failures, classification changes, etc.).

4. Policy decisions (data and service access) were made based on role, clearance, and citizenship user attributes in the Lightweight Directory Access Protocol (LDAP) directory (that were tied to the identity token/PKI certificate) using the security services.

The definition of DAC+ evolved throughout the development cycle, as the engineers refined the requirements and developed workable solutions. As a result, the coding requirements changed, as well as the test cases to verify/validate capability. Also, some challenges encountered in implementing the DAC+ requirements involved legacy back-ends and data sources. Many back-end databases did not have provisions to support DAC+ requirements (e.g., data labeling). The vastly different types of data types and data stores made a singular approach to data labeling unrealistic.

Coding DAC+ standards is a complex task and requires significant security engineering to perform. The standards and practices will continue to evolve for some time as new technologies are put in place and as DAC+ grows into Risk Adaptive Access Control (RAdAC). This migration will not occur with the flip of a switch. A phased implementation approach which supports a hybrid environment of legacy and RAdAC implementation is key to the success of the SOA.

Legacy data sources, in general, do not label data. Labeling means binding classification and releasable information to the data (i.e., non-repudiation). Each legacy data source/service will need to develop a low-risk/impact incremental implementation to support the larger community as the community approaches future Net-Centric IA control mandates.

Recommendations

Review current accreditation guidance documents for required revisions to support an information sharing (SOA) environment.

Refine further auditing guidelines and coordinate requirements with DCID and other security policy mandates. Develop specifications for an enterprise auditing services, rules for releasability of audits, and discovery and access of audit logs.

Programs of record need to start labeling current data now with classification and releasability metadata tags.

Observation and Analysis

The Horizontal Fusion Security Policy Working Group objective included preparing a challenge to the usage of MAC and labeling requirements. The policy challenge would have centered on the usage of PKI and Metadata tags for information storage. Horizontal Fusion targeted security requirements:

- Based on DCID 6/3 and DoD Instruction (DoDI) 8500.2
 - For DoDI 8500.2, the goal was to meet Mission Assurance Category II and Confidentiality Level High requirements
- Policy Guidance for the use of Mobile Code Technologies in DoD Information Systems

Challenging Security Policy is a slow process. To protect information and manage risk, it was important for the Portfolio to work within the bounds of existing policy while demonstrating that an SOA provides Net-Centric IA when combined with a risk management approach. Policy challenges were not put forward due to the delay in the technical specification and implementation of DAC+ across the Portfolio, executing a security infrastructure, and the sheer effort required to account for metadata tagging and classification handling.

Recommendation

Specific policy implications must be identified and addressed as they pertain to an SOA in the C&A process. A roadmap approach must then be developed for each Portfolio security area. Establish liaison relationships with external organizations and community working groups to coordinate and socialize SOA needs and proposed policy changes.

4.1.2 Certifying and Accrediting a Services-Oriented Architecture (SOA) and Defining Discretionary Access Control-Plus (DAC+) Requirements

Observation and Analysis

To achieve cross-domain information exchange objectives, the Horizontal Fusion Portfolio targeted DCID 6/3 PL-5 requirements. The Portfolio developed the following key requirements to move information across domains without a human reliable review process and referred to them as DAC+.

Each data object within the Collateral Space is required to have:

1. A metadata tag that contains a security classification attribute
2. A digital signature applied
3. An auditable metadata tag change process
4. An NCES Policy Decision Server and Extended LDAP containing a Trusted Source of Security Clearance Information
5. Data objects that use the security classification for access control through the Role-Based Access Control (RBAC) Filter

Leadership is a key ingredient of what was done well. The Portfolio Manager's vision challenged the Portfolio Initiatives to "aim for PL-5" but apply Net-Centric concepts as the driver to getting Portfolio Initiatives to think "outside of the box" and battle "business as usual". Defense Information Services Agency (DISA), responsible for supporting the Portfolio with core enterprise services, presented the preliminary concepts for a Net-Centric security architecture and security services that had a solid "feel" or solution to support cross-domain information exchange, role-based access, etc. The challenge for the Portfolio was its aggressive schedule to deliver a cross-domain information exchange solution, compared to the uncertainty of whether or not security services would be delivered by DISA to meet that schedule. Though there was a "wait and see" attitude exhibited by some Portfolio Initiatives, the Portfolio Manager never relented in the requirement to implement DAC+ features within the original schedule constraints. The outcome was a success. Other contributing leadership factors included:

- **A Single DAA.** A Single DAA provided a single point of reference for Portfolio Initiatives and Partners. The DoD CIO said in his designation letter, "In order to best ensure that a risk management perspective to the information assurance of this Net-Centric Initiative is implemented, an enterprise approach will be taken." This process allowed for consistent guidance across the Portfolio without allowing service/agency/command-specific requirements to cloud the development effort. Local commands were coordinated with and issues were evaluated for adoption or rejection by the Portfolio's single DAA. The fielding of providers, at disparate locations, could have derailed the capabilities of the entire Portfolio to meet local requirements. The single enterprise DAA process was a success.
- **Lead by example.** The selection of Portfolio Initiatives, with potential cross-domain or secure wireless solutions as part of their capability, was important to overcoming technical obstacles. Portfolio Initiatives with previous experience in the Horizontal Fusion Portfolio contributed to the Initiatives' tenacity and synergy of security engineering expertise to define solutions in a schedule-driven environment.

- **Accountability.** Portfolio Initiative Program Managers were held accountable for certifying that various tasks were completed to support the Interim Authority To Operate (IATO). The C&A Team supported the Portfolio Initiatives with guidance and advice, but held them accountable for being prepared for testing. In addition, the C&A Team continuously evaluated Portfolio Initiatives for security knowledge, documentation readiness, schedule, technical solutions for advanced features, and testing.

Technical solutions for the design, development, test, standup, and approved functional enterprise infrastructure to implement the DAC+ features were delayed until almost the end of May 2004 for the entire Horizontal Fusion Portfolio. The primary reason for the delay was uncertainty associated with NCES security services delivery and its content. The lack of a security engineer for the enterprise also contributed to this delay. With no firm enterprise architecture or infrastructure solution early in the process, most Portfolio Initiatives resorted to simply guessing or creating solutions “on-the-fly.”

Recommendation

In preparation for future capability demonstrations, and in preparing newly acquired Portfolio Initiatives for initial system security and functional testing, an approved and functional enterprise design structure should conceivably be accomplished **within the first 60 days of their initiation.**

Include security in all system requirements from the very beginning. Create the Security Requirements Traceability Matrix (SRTM) early-on, and use it to perform a local Risk Assessment (RA). Coordinate results of the RA with system security administrators and system developers and engineers. This will provide a better understanding of the threats/vulnerabilities unique to their system(s) and why protection is necessary. Each Portfolio Initiative should acquire the services of a knowledgeable system security engineer during system development.

Observation and Analysis

The Portfolio managed to successfully accomplish DAC+ testing within a rigid schedule. A wealth of lessons learned emanated from the C&A process. The most significant lessons learned revealed that the Portfolio Initiatives’ security test evaluation plans and procedures were not as comprehensive as needed and were not consistent across the Portfolio. Success depended in part on the quality and maturity of security engineers employed by each Initiative and subsequently produced test plans that focused on advanced security features to support DAC+. The C&A Team assembled test procedures from successful Portfolio Initiatives in an effort to facilitate the synergistic effects of collaborating and sharing test plans and procedures across the Portfolio. The Portfolio could have benefited a great deal more from of this type of effort.

Even though automated test procedures used to check security configuration settings remained consistent across the Portfolio, the unique security of FY2004 needed consistent repeatable procedures for those features.

Recommendation

The Security Policy Working Group should establish Sub-working Groups to create unique test procedures against the requirements. These Sub-working Groups can be assigned by operating system and a small subset of the requirements. By assigning the effort to smaller working groups, two things can be accomplished, repeatability and relevant test procedures.

Observation and Analysis

Planning shortcomings were also revealed in a single date for the SSAA documentation delivery near the end of the Portfolio Initiatives' development lifecycle. This single date did not allow for the identification of security problems early in the development.

Security fixes identified after the fact required extensive use of manpower to retrofit portlets and portal architecture. The retrofits caused other services to become compromised and required reengineering of the solutions.

Recommendation

Develop a three-phased approach to develop the SSAA. This will allow problems to be identified early in the development of the portal and portlets.

4.1.3 Cross-Domain Information Exchange

In a truly Net-Centric environment, the seamless sharing of information across domains is a vital capability bringing information to the edge-user. In an SOA, the protection of information moves from the network boundary to the entire network as all entities are involved. For FY2004, the Portfolio developed cross-domain solutions for the one-way Unclassified-to-Secret flow of battlefield perishable information into the Collateral Space and the Coalition-to-Secret flow of the North Atlantic Treaty Organization (NATO) Secret information into the Collateral Space. These solutions incorporated the use of labeled data, strong identity management, digital signatures, role-based access controls, and intelligent boundary devices as needed to protect the domains from unauthorized, non-Horizontal Fusion users.

4.1.3.1 Technical Approach

Observation and Analysis

Efforts were made to involve other entities throughout the cross-domain community in the Horizontal Fusion cross-domain efforts. Personnel from the National Security Agency (NSA) did participate in several workshops. This participation, though, was primarily as observers and not participants. Additionally, different personnel came to each workshop. There was no participation from the DISA Cross-Domain office or the service cross-domain offices.

Recommendation

Establish liaison relationships with external organizations such as NSA customer advocacy office, DISA/NSA cross-domain working groups, Joint Staff, and Services cross-domain services offices. Participate in their working groups to coordinate and socialize Horizontal Fusion needs and proposed solutions.

Observation and analysis

It became obvious as the year unfolded that Horizontal Fusion had several issues concerning Net-Centric cross-domain solutions. Current cross-domain technology is point-to-point with known participants. Net-Centric architectures are all about ad hoc information and data discovery. However, the current architecture of SIPRNet, the backbone infrastructure for Horizontal Fusion, does not routinely employ the security features built into the Collateral Space (PKI, data labels, role-based access controls, access attributes, etc.). This caused Horizontal Fusion to establish a cross-domain information exchange solution set that ensured protection for SIPRNet in its current configuration and was approved by the DSAWG.

Recommendation

When building a new architecture using an old infrastructure, the security limitations of that old infrastructure and its environment must be understood and preparations to provide appropriate interim controls must be considered.

Observation and Analysis

The SIPRNet infrastructure with its System-High mode of operation lacked the necessary security controls to allow the use of the Horizontal Fusion cross-domain solution goal, especially in a two-way flow. A decision was made to exercise the cross-domain solution goal with a simulated Coalition network on the SIPRNet. This decision allowed Horizontal Fusion to gather data on the Net-Centric approach to cross-domain information exchange that was implemented without risk to the SIPRNet.

Recommendation

Simulation is a good way to test solution goals when the existing infrastructure and environment cannot be trusted.

Observation and Analysis

During the later part of the year, a decision was made to take a two-prong approach to developing the technical solution for cross-domain. The first prong was to look ahead to the future to the solution goal and develop a roadmap to get there. The second prong was to develop a near-term solution for the one-way Unclassified-to-Secret and the Coalition-to-Secret flows. Although initiated, this strategy did not work well as the near-term need to include the connection approval process soon overwhelmed the Cross-Domain Information Exchange Team.

Recommendation

The Horizontal Fusion Cross-Domain Information Exchange Team needs to maintain a focus on achieving the goals as established in the GIG Information Assurance Architecture. Horizontal Fusion needs to continue to solve problems and implement solutions that emphasize the value and potential of: 1) User Authentication via PKI Certificates; 2) Policy Decisions using Core Enterprise Services-Security Services; and 3) Role/Clearance/Citizenship-based Access within the Enterprise. Horizontal Fusion should pass network-to-network cross-domain problems to the DoD cross-domain community for them to solve.

Observation and Analysis

The Cross-Domain Information Exchange Team initially centered their efforts on facilitating the Portfolio Initiatives through the process of identifying their cross-domain requirements, coming to consensus on a common solution for common requirements, and then working with one Portfolio Initiative to develop the solution for use by all. However, many Portfolio Initiatives did not understand their role in this process and resisted. Many Portfolio Initiatives believed that the solutions needed for cross-domain information exchange would be provided to them. In addition, the Portfolio Initiatives generally lacked dedicated security engineering expertise, especially in cross-domain. Lacking organic security engineering expertise resulted in significant time spent in Working Group meetings educating the Portfolio Initiatives on the requirements and delays in development of solutions. The Portfolio Initiatives looked to the Horizontal Fusion Portfolio Management Team for assistance in resolving day-to-day engineering challenges. In an attempt to resolve this situation, Portfolio Initiatives were strongly encouraged to acquire the missing security engineering expertise.

Recommendation

All Portfolio Initiatives need access to security engineering support. Portfolio Initiatives should acquire their own dedicated support. In addition, the Horizontal Fusion Portfolio Management Team should have a security engineering lead to oversee the security engineering efforts and provide assistance to Portfolio Initiatives as needed.

Observation and Analysis

Some code used in Horizontal Fusion came from non-U.S. sources. Many commercial-off-the-shelf (COTS) software packages contained code developed overseas. In addition, some services created for some of the Portfolio Initiatives was written by non-U.S. personnel.

Recommendation

Coordinate with appropriate sources and determine if the COTS or service code produced and used in Horizontal Fusion should be evaluated or reviewed to ensure there is no malicious content. Policy needs to be changed to clarify guidance as to the use of code generated by non-U.S. personnel.

4.1.3.2 Policy Areas

Observation and Analysis

Due to changing requirements and the flux in the Portfolio Initiatives' technical solutions, cross-domain information exchange requirements were not defined until March 2004. The existing SIPRNet connection approval process is complicated, iterative, time consuming, and supports only point-to-point solutions. This was a significant challenge given the Horizontal Fusion SOA and the inflexible schedule requirements required for Quantum Leap-2. Horizontal Fusion accepted this challenge, constantly striving to find ways to streamline the process. This willingness to innovate was recognized by the DSAWG. DSAWG members suggested that Horizontal Fusion be used as a prototype to test ways to make the process more efficient. One of these efficiency methods was the concept of NSA participation with Horizontal Fusion security testing of its cross-domain solution instead of separate testing by an NSA Test Team. Other efficiencies included the consolidation of Horizontal Fusion cross-domain instantiations into one consolidated package. There was a single Horizontal Fusion Portfolio Management Team Lead that was responsible for managing the combined package through the connection approval process. This centralized role in the DSAWG approval process went well. The single voice to the DSAWG eased the confusion and facilitated the process. Interaction between the Horizontal Fusion Portfolio Management Team Lead and the Certification Team Lead went very well as they worked together to solve the problem.

It takes significant time and effort and, potentially senior level involvement, to change existing policies and procedures. Centralized processing of the connections approvals is a must. Increased liaison with the external interested stakeholders would be helpful.

Recommendations

NSA, DSAWG, and the SIPRNet Connection Approval Office (SCAO) continue to use Horizontal Fusion as a prototype to test ways to streamline and make the approval process more efficient. Work not only on ways to streamline the current process, but think “out of the box” to create new procedures or to recommend policy changes that will streamline the process, (i.e., a single approval for multiple instantiations).

In parallel to developing policy recommendations, continue to follow the established procedure in order to ensure successful completion and to gather data on where the process can be made more efficient and responsive.

Specifically relating to the connection approval process, involve DSAWG, SCAO, Joint Staff, and applicable Service Representatives early and keep them informed to preclude issues of procedure and ownership.

4.1.4 Secure Wireless Communications

Secure Wireless efforts for FY2004 concentrated on the secure use of commercial wireless technologies to expand the reach of the Collateral Space to the edge-users in deployed locations. These connections were used in the classified and unclassified environments to provide a mobile data collection capability to the Collateral Space.

4.1.4.1 Technical

Observation and Analysis

Some Portfolio Initiatives failed to realize that secure wireless was multifaceted, thus they did not comprehend that they had a need for a secure wireless solution. Several Portfolio Initiatives were identified as Secure Wireless solutions later in the year.

Recommendations

All Portfolio Initiatives should be educated early in the process as to requirements and definitions of technologies. Specific guidance will provide clarity for all Portfolio Initiatives to identify their specialized needs.

4.1.4.2 Policy

Observation and Analysis

The NSA policy for use of the Advanced Encryption Standard (AES) cryptography for the protection of classified information (and connectivity to SIPRNet) was unclear and easy to misinterpret, which led to delays. The final understanding of this policy revealed that,



although the AES 256 algorithm was approved for use to protect classified information, NSA requires each implementation to undergo a detailed review and approval process.

Recommendations

Participation in the Horizontal Fusion Secure Wireless Sub-working Groups by knowledgeable NSA staff would be a benefit to explain their policies and procedures.

Engage the various approval organizations early and have them involved in the plans for use of cryptographic algorithms.

Designate an individual to solely concentrate on IA policy to: 1) analyze existing policy, 2) provide guidance to the Portfolio Initiatives, and 3) forward recommended policy modifications that will ensure data security while facilitating implementation of an SOA. Recommend NSA streamline the process for approving each implementation of the AES 256 algorithm.

Observation and Analysis

Security policy for the use of commercial wireless technologies in a DoD environment, DoD Directive (DoDD) 8100.2, was issued late in the year. Analysis of its requirements and discussion with the policy creators revealed that this policy addressed the use of commercial wireless in DoD, but not in the “tactical” environment. No current policy exists that applies to use of commercial wireless in a DoD tactical environment.

Recommendation

A policy for use of secure wireless commercial technologies in a tactical environment needs to be produced.

4.1.5 Public Key Infrastructure (PKI) Certificates

The Horizontal Fusion Portfolio leveraged DoD PKI on SIPRNet to identify end users (client), service providers, and service required mobile code. The DoD SIPRNet PKI certificates, be it client, server, or code signing, constitute the building blocks of IA in an SOA. One of the unique capabilities that DoD SIPRNet PKI provides is an ability to accomplish single sign-on. Current SIPRNet PKI policy will require discussion and clarification before DoD PKI can truly impact and improve Net-Centric warfare.

Overall, the Horizontal Fusion use of the DoD PKI was a success, as demonstrated in Quantum Leap-2. However, the Horizontal Fusion Portfolio experienced difficulty in 1) obtaining client certificates through the SIPRNet PKI Local Registration Authority (LRA); 2) defining the issuance process; 3) obtaining SIPRNet mobile code certificates; and 4) implementing SIPRNet server certificates. The robustness of the Non-Secure Internet Protocol Router Network (NIPRNet) PKI processes helped in addressing emerging or otherwise immature SIPRNet processes.



In addition to the DoD certificates, Horizontal Fusion leveraged the Joint Interoperability Test Command (JITC) certificates. The JITC proved to be a valuable resource for obtaining NIPRNet PKI certificates for development and test purposes quickly. The use of JITC certificates led to the overall success of the test and integration of the Horizontal Fusion Portfolio web services.

4.1.5.1 Certificate Use Policy

Observation and Analysis

The current physical handling of SIPRNet PKI client certificates is difficult due to ambiguity in the definition of the classification level of the actual certificate. The DoD PKI Certificate Registration Instruction (CRI) is labeled For Official Use Only (FOUO), is time sensitive material, and contains the initial User Number and Access Code. To take possession of the certificate, the user is instructed to download the certificate and save the certificate to a floppy disk. This action is part of the security debate; as the classification level of the certificate contained on the floppy disk is undefined. The actual certificate is password protected and if the user loses the password or mistypes the password three times, the certificate is revoked and an LRA must intervene to reissue.

Furthermore, steps need to be taken to adopt Common Access Card (CAC) at the SIPRNet level. The floppy disk does not represent a viable conduit to transfer the client certificate. Horizontal Fusion Quantum Leap-2 demonstrated the use of SIPRNet PKI to the warfighter. Feedback from these warfighters indicated that floppies in the field are not viable and that they would prefer to use their CAC.

Recommendation

Declare the classification of the SIPRNet PKI certificate as FOUO. Adopt CAC as the preferred method of holding and presenting the PKI Client Certificate at the SIPRNet level.

Observation and Analysis

In the process of delivering a SOA, Horizontal Fusion determined that certain implementation testing needs to occur on the SIPRNet before web services are made available to the warfighters. For example, to properly implement single sign-on, Role-Based Access, and NCES Security Services, it was necessary to test these capabilities and services on the SIPRNet. This testing was limited due to the fact that a test batch of PKI certificates, such as the JITC test certificates used on the NIPRNet, were not available on the SIPRNet. Allowing a JITC Trusted Root Certificate Authority to exist on SIPRNet is needed for better integration of web services and would yield the same benefits as seen on the NIPRNet.

Recommendation



Issue policy that allows JITC Certificates to be a Trusted Root CA on SIPRNet.

Observation and Analysis

The DoD PKI does not support inter-agency Trusted Root CAs. This means that DoD does not recognize PKI certificates from any organizations outside DoD. Therefore, organizations conducting business within the DoD must also be issued DoD certificates. This past year, Horizontal Fusion sought and received from the DoD PKI Program Office, the ability for the Department of State (DoS) to obtain DoD PKI certificates. This paved the way for DoS to participate in Quantum Leap-2 and allowed for DoS data holdings to be exposed to the Collateral Space.

Recommendation

Leverage the work started by Horizontal Fusion to begin working inter-agency Trusted Root CA issues. Begin to establish policies between DoD and known inter-agency departments (DoS, Intelligence Community, etc.) that will allow those agencies to work with their own PKI Certificates and still be able to share information via the SIPRNet.

DoD services should identify these Certificate Authorities as valid and render services subject to the RBAC policies and attributes that pertain to those certificates.

Observation and Analysis

As policy is defined to allow inter-agency Trusted Root CAs, policies must also be defined that will allow Coalition Partner PKI certificates to be leveraged. Horizontal Fusion forged the path for DoS to obtain DoD PKI certificates. The next hurdle will be to adapt policy for Coalition Partners. The Portfolio Initiatives determined that only through local sponsorship could foreign national Coalition representatives be granted a DoD PKI certificate. A model that would leverage NATO and Coalition Partners Trusted Root CAs may prove more effective.

Recommendation

Leverage the work started by Horizontal Fusion to begin working Coalition Trusted Root CA issues. Begin to establish policies between DoD and known Coalition partners (NATO, Commonwealth, etc.) that will allow these partners to work with their own PKI Certificates and still be able to share information.

4.1.5.2 Certificate Issuing Process

Observation and Analysis

PKI proved to be a powerful tool to establish strong identity and Horizontal Fusion leveraged the SIPRNet PKI to certify the identity of web services, mobile code, and the identities of *Mars* Portal authorized clients. The processes to obtain the DoD SIPRNet PKI certificates proved to be immature and arduous.

Members of the DoD PKI Program Office provided initial guidance early in the Horizontal Fusion development cycle. This guidance primarily targeted the web services development community and provided URLs for developers and managers to use as a guide for the issuing process. The DoD PKI Program Office staff also provided some guidance for client certificate acquisition. The Portfolio Initiatives used the provided guidance, but had difficulty in determining the proper LRA that would provide the proper certificate registration. The current SIPRNet PKI LRA support community is too small to support a diverse DoD/Joint Command/Service group that is focused on development, test, and integration. The current LRA group is not able to support any type of deployment operations. Of particular distress is the lack of an automated LRA identifier. An overarching directory of LRA contacts is available but is inadequate to identify appropriate SIPRNet LRAs, who are different from the more numerous NIPRNet LRA group. The established directory cannot search or collate by location, service branch, or network. The Navy LRA support at SSCC proved up to the task of serving the local Horizontal Fusion requirements. Using other LRA support proved difficult. Horizontal Fusion leveraged the PKI Help Desk located in Oklahoma City to get LRA contact information and guidance. This facility provided expert assistance in matching specific Portfolio Initiatives and their requirements to the correct available LRA.

Recommendation

Improve the LRA web look-up tool administered by the DoD PKI Program Office. Include location and service branch look-ups. Include specific tools to help locate a SIPRNet LRA. Greatly augment the current SIPRNet LRA pool.

Observation and Analysis

An important aspect of successfully issuing PKI certificates lies in providing ample lead-time before the PKI certificate is required. Often the PKI acquisition process requires weeks of lead time—identifying the client or server requirements, contacting the specific LRA, providing the LRA requested certificate requests, making the face-to-face required issuance, then finally installing the certificates.

Recommendation

Provide ample lead-time before a PKI certificate needs to be utilized. The PKI Program Office needs to produce a PKI user guide and “How To Guide for PKI” as well as promote the established PKI web site to educate consumers.

Observation and Analysis

Several Horizontal Fusion Portfolio capabilities utilize mobile code. Mobile code requires identity just as services and clients require identity. When mobile code was first introduced by the Horizontal Fusion Portfolio capabilities, there did not exist a PKI certificate to identify and authenticate it. Through Horizontal Fusion, the SPAWAR Test and Integration Team forged ahead and obtained the first PKI certificates for mobile code on SIPRNet by authorization of the SPAWAR Base Commanding officer. The process by which SPAWAR obtained their certificates followed the same procedure as NIPRNet and the first certificates were issued from the NIPRNet CA. The two code signing certificates issued for the Horizontal Fusion Team are numbered 1 and 2 for the entire U.S. Navy. Part of the process Horizontal Fusion instituted to issue a mobile code certificate included scanning for malicious code using standard industry tools and practices; but no code analysis was conducted.

Recommendation

SIPRNet deployed mobile code should employ requirements and specify tools for code analysis.

4.1.5.3 Technical Implementation Issues

Observation and Analysis

There is only one Trust Store available on SIPRNet that maintains the CRL. Net-Centric operations will require that multiple Trusted Root CA CRLs be called to be able to verify inter-agency identity and access Coalition CAs, which are key to cross-domain information exchange.

Recommendation

Allow multiple Trusted Root Certificate Authorities CRLs, to include inter-agency (i.e., DoS) and Coalition partners. Ultimately, the SOA should be able to access these CRLs regardless of the domain in which they reside, but short-term bridging solutions (i.e., SIPRNet to Coalition) and trust relationships need to be developed to support cross-domain information exchange.

Observation and Analysis

Because of the difficulty associated with acquiring the DoD SIPRNet PKI certificate, portability of the certificate from server to server, as a web service matures and web service utilization expands and contracts, becomes an issue. Associating the services with a certificate that may deploy across a server farm is a better approach than assigning a unique certificate to each individual server that supports the web service. Leveraging the JITC certificate in the development of a web service allows for the initial scope of server support, but once the web service is placed into production, the DoD certificate is required and the DoD certificate poses administration limitations, primarily in acquiring the certificate in a timely manner, but also in the flexibility of balancing hardware and associated certificates with the web service call demand. If identity is placed at the web service level, greater flexibility in the administration of the web service may be afforded.

DoD CA keys are not embedded into the browsers currently deployed and developed within DoD. If the DoD Root CA public keys were embedded, administration overhead would be less. The major browser vendors need to provide default DoD Trusted Root CAs. In the near-term, Horizontal Fusion, as well as other DoD Net-Centric endeavors, will benefit by developing and embedding tools to facilitate DoD Trusted Root CAs.

Recommendation

Certify identity at web service level. Provide means to allow default DoD Trusted Root CAs.

Observation and Analysis

The current Java Runtime Environment (JRE) Plug-Ins expose the client PKI password in a clear text format. The JRE is required by many web services. When the password is exposed, the client identity is jeopardized. Clear text password vulnerability will limit the security accreditation of web services presented by the JRE. Sun Microsystems developed and distributed the Java JRE and must pursue a solution to eliminate exposing the password.

Recommendation

DoD must pursue a solution to eliminate exposing the password in the JRE graphical user interface (GUI) to ensure security accreditation of web services.

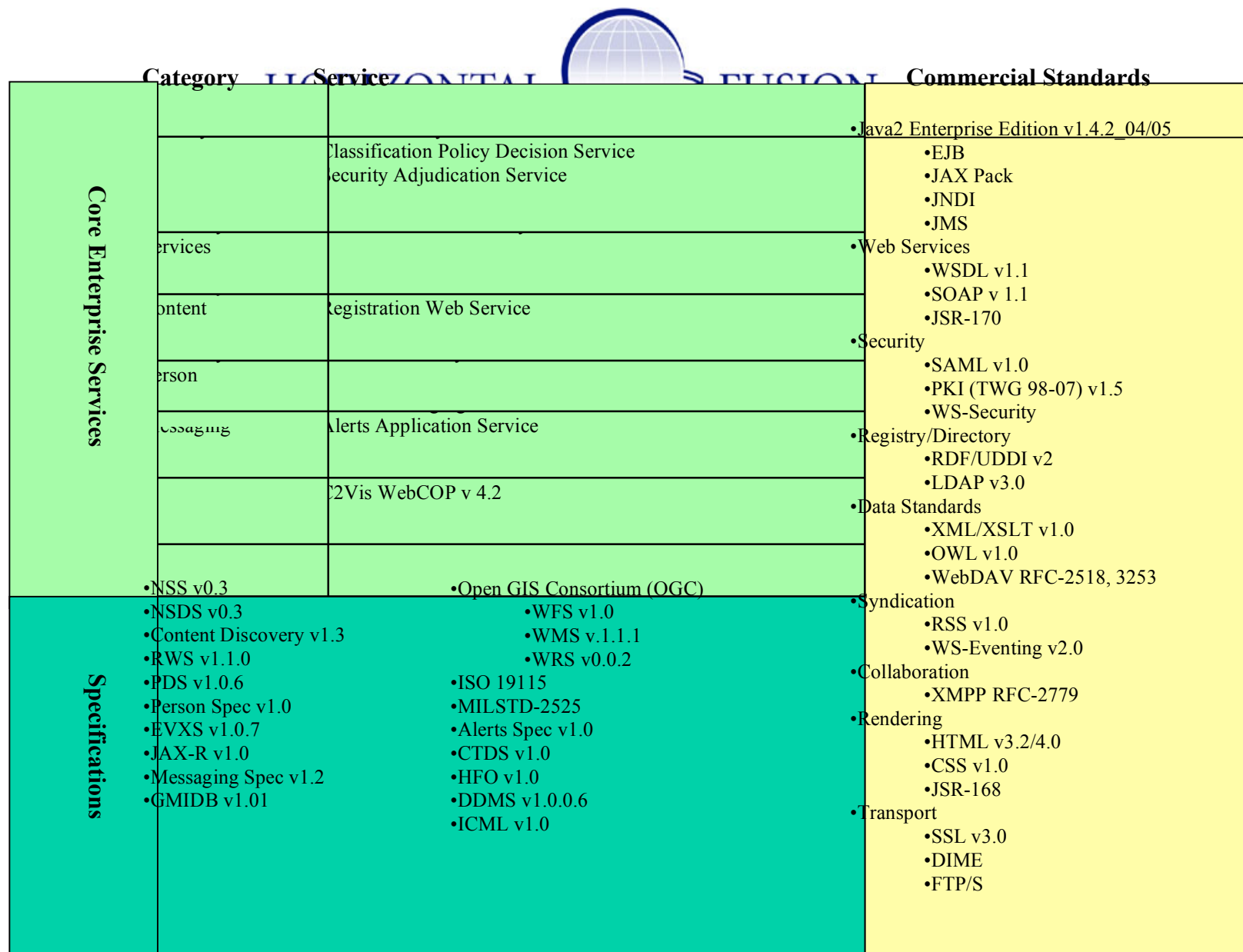
4.2 Standards and Specifications

At the enterprise level, Horizontal Fusion provides a high return for a relatively low investment by providing a SOA environment that legacy programs can attach to while new capabilities are developed to ingest it naturally. The evolutionary approach minimizes the cost of transitioning to a net-centric mode of operations. The Horizontal Fusion Portfolio neither produces requirements nor standards; but, instead, implements an SOA environment in accordance with the existing requirements of the Global Information Grid and the published standards of



standards organizations. Horizontal Fusion provides both data and IA standards implementation and feedback, although, at this point, the feedback process lacks formal documentation.

Published standards implemented this year include the Defense Discovery Metadata Specification (DDMS), NCES, and those standards of the Intelligence Community Metadata Working Group (ICMWG) as well as existing COTS and Government-off-the-shelf (GOTS) standards. The Horizontal Fusion SOA architecture employs industry standards such as XML, JSR168, SOAP, Web Services Descriptive Language (WSDL), etc. Furthermore, Horizontal Fusion has led the charge in defining specifications where no COTS or GOTS standard existed. The Person Specification and Track Specification are examples of products that have been developed for DoD in support of the Horizontal Fusion Portfolio. Figure 2 is a chart detailing the services, standards and specifications used by Horizontal Fusion in FY2004.



The diagram illustrates the relationship between Core Enterprise Services, Specifications, and Commercial Standards. It is structured as a table with three main columns: Category, Service, and Commercial Standards. The 'Core Enterprise Services' section is highlighted in light green, 'Specifications' in light blue, and 'Commercial Standards' in light yellow.

Category	Service	Commercial Standards
Core Enterprise Services		<ul style="list-style-type: none"> •Java2 Enterprise Edition v1.4.2_04/05
	Classification Policy Decision Service	<ul style="list-style-type: none"> •EJB •JAX Pack •JNDI •JMS
	Security Adjudication Service	
	Services	<ul style="list-style-type: none"> •Web Services •WSDL v1.1 •SOAP v 1.1 •JSR-170
	Content	<ul style="list-style-type: none"> •Security •SAML v1.0 •PKI (TWG 98-07) v1.5 •WS-Security
	Person	<ul style="list-style-type: none"> •Registry/Directory •RDF/UDDI v2 •LDAP v3.0
	Messaging	<ul style="list-style-type: none"> •Alerts Application Service •Registry/Directory •RDF/UDDI v2 •LDAP v3.0
		<ul style="list-style-type: none"> •C2Vis WebCOP v 4.2 •Data Standards •XML/XSLT v1.0 •OWL v1.0 •WebDAV RFC-2518, 3253
Specifications	<ul style="list-style-type: none"> •NSS v0.3 •NSDS v0.3 •Content Discovery v1.3 •RWS v1.1.0 •PDS v1.0.6 •Person Spec v1.0 •EVXS v1.0.7 •JAX-R v1.0 •Messaging Spec v1.2 •GMIDB v1.01 	<ul style="list-style-type: none"> •Open GIS Consortium (OGC) •WFS v1.0 •WMS v1.1.1 •WRS v0.0.2 •ISO 19115 •MILSTD-2525 •Alerts Spec v1.0 •CTDS v1.0 •HFO v1.0 •DDMS v1.0.0.6 •ICML v1.0
		<ul style="list-style-type: none"> •Syndication •RSS v1.0 •WS-Eventing v2.0 •Collaboration •XMPP RFC-2779 •Rendering •HTML v3.2/4.0 •CSS v1.0 •JSR-168 •Transport •SSL v3.0 •DIME •FTP/S

Figure 2 Horizontal Fusion Services, Standards, and Specifications

4.2.1 General

Vendor implementations of different commercial “standards-based” software tools are not always compatible. There are issues with vendor compliance with the standard as well as vendor-to-vendor interoperability. Some of the inconsistencies are due to the fact that the implemented standards are new and vendor implementations are immature. Developers encountered challenges in these areas:

- Web services (due to the differences between operating systems such as Axis, Glue, WASP and .NET)
- Portal JSR-168 standard (with the differences between vendors such as BEA and PLUTO)
- Web Services for Remote Portals (WSRP), SOAP, UDDI, and XML

Recommendations

Aggressively review and assess which standards should be used and evaluate vendor implementations and usage. Engage and leverage the entire DoD Net-Centric community to get selections made and guidance issued.

4.2.2 Taxonomy/Ontology

A taxonomy is a hierarchical means of classifying data. An ontology is a formalized, semantically richer taxonomy. While a taxonomy is a tree with limited relationships between concepts, an ontology is a web that allows the specification of more complex relationships between concepts.

Observation and Analysis

The Horizontal Fusion data providers collaborated on a discovery taxonomy. This taxonomy was provided to the ASD/NII Taxonomy Focus Group and became the basis of ASD/NII’s core taxonomy. The core taxonomy serves as a hub for the DoD taxonomy framework. Community of Interest (COI) taxonomies are currently being plugged into this framework to provide an extensible DoD taxonomy.

In Horizontal Fusion, data providers registered their data content/data sources based on the structure of the taxonomy. The Federated Search routes queries to appropriate data sources based on their registration. The data source registration capability succeeded. Data sources registered into the taxonomy allowed searches to be directed to the correct data providers increasing the quality of responses and decreasing the quantity of responses. However, taxonomic registration needs to be fine-tuned. It will be necessary to enhance, augment, or modify the current taxonomy to encompass other COIs and their data sources. Given the potential for high network load, it is imperative that the Federated Searches be more accurately directed to data providers.



The taxonomy is also used for the categorization of search results. The Visbee portlet (visualization tool within Federated Search) allowed users to view search results based on concept and successfully demonstrated how a taxonomy can help make semantic sense of disparate data.

Recommendations

Future work in this area should concentrate on establishing the correct level of taxonomy granularity for registration that will yield the best performance and search accuracy.

Observation and Analysis

In Horizontal Fusion, the ontology is used as part of the query refinement process. The refinement engine translates query keywords into ontological concepts and expands the query accordingly. This allows Federated Search to send a query to a data source that has registered concepts related to the keywords.

Horizontal Fusion has started the migration from a taxonomy to an ontology by mapping ASD/NII's Core Taxonomy into a Defense Advanced Research Projects Agency (DARPA) developed ontology known as Cyc. The mapping will provide a semantically richer environment that can be used for registration, query refinement, and content discovery. This mapping is a decisive step towards interoperability with other taxonomies generated by other government organizations, other COIs, and coalition and allied partners. The Cyc ontology was chosen because it is large, reliable, and quite salient to warfighter interests. It also allows for web deployed, sharable ontology-based discovery tools on all government networks (Joint Worldwide Intelligence Communication System (JWICS), SIPRNet, NIPRNet).

Recommendations

Expand the core taxonomy to include ontology of data and information.

Enhance the Federated Search implementation to use a semantically rich ontology to make data discovery smarter and more robust to ensure returned results most closely match the request of the user.

4.2.3 DoD Discovery Metadata Standard (DDMS)

The DDMS is a metadata tagging system that has arisen out of the DoD's Net-Centric Strategy. Metadata is data that defines and categorizes other, lower level data. It is data about data. The strategy is to define a flexible and general set of metadata specifically geared to the DoD's usage and needs, and then to allow COIs to expose their data via well-accepted metadata tags. Data sources and data consumers are no longer required to create a point-to-point communication in order to exchange information. Instead, DDMS permits an SOA architecture to arise where the categories of possible data types are known in advance by nodes within the DoD network.

Observation and Analysis

A key advantage to the employment of DDMS in a Net-Centric architecture is that it allows data to be accessed and used by unanticipated users. Data is exposed using DDMS without regard for the end-user. This places the responsibility for data-generation and metadata tagging solely on the Data Provider. A Data Provider will certainly include various defense communities (or COI) that define the lower level data that is collected and exposed. Thus, standardization of the data can occur by common agreement within that community; all that is required at the global level is that a common set of metadata is used to describe the standardized data. The Intelligent Federated Index Search (IFIS) normalizer of the Federated Search engine in Horizontal Fusion uses DDMS defined semantics to represent the query. This provides a commonality of meaning across all parts of the Federated Search System.

As the standard for DoD discovery, DDMS was incorporated into the Federated Search Web Service (SWS). The Federated Search normalizer uses DDMS defined semantics to represent the query. However, there was no DDMS XML schema. ASD/NII chartered the DDMS Schema Focus Group to provide a usable XML schema. Horizontal Fusion implemented the alpha version of the XML schema for Quantum Leap-2 and proved that DDMS is a viable means of describing content discovery queries and results.

DDMS XML schema version 1.0 alpha incorporated IA Information Security Marking v1.0 (ISM 1.0). ISM 1.0 contained bugs and/or obsolete Intelligence Community Controlled Access Program Coordination Office (CAPCO) guidance, which proved an issue for Horizontal Fusion. These deficiencies have been addressed in ISM 2.0.

Recommendation

The DDMS Focus Group should upgrade the XML schema to include ISM 2.0 standards and publish it to the DoD Metadata XML Registry.

Observation and Analysis

Horizontal Fusion has a number of data provider and consumer requirements that need Federated Search to be able to support location-based queries. The DDMS schema used by Horizontal Fusion provides very little support for geospatial information. National Geospatial-Intelligence Agency (NGA) is now collaborating with DDMS to augment the geospatial tags.

Recommendation

The DDMS Focus Group should continue to work with NGA to include/extend geospatial aspects within the specification and publish it to the DoD Metadata XML Registry.

4.2.4 Person Data Specification



The Person Data Specification is an XML Schema which is suitable for transport between systems using web services. The Person Data Specification will allow, through the use of Federated Search, the Non-Obvious Relationship Awareness (NORA), and the Visualization/Information Dominance (V/ID) Portfolio Initiatives, the user to discover relationships and linkages of people to other critical intelligence. As Horizontal Fusion continues to expand upon the specification and integrate it with other ongoing efforts, this utility will grow exponentially.

Observation and Analysis

The Horizontal Fusion Portfolio recognized the need to standardize biographic/biometric data exchange standards to enhance knowledge discovery/mining by specific Portfolio participants. In an attempt to facilitate the flow of biographic/biometric information, Horizontal Fusion combined the efforts of the ICMWG, NORA, and the Virtual Knowledge Base (VKB) to meet this goal. The Horizontal Fusion data providers collaborated on a specification to share person data. The specification combined and extended the work of the Intelligence Community Terrorist Watchlist Person Data Exchange Standard (TWPDES) group and the work done in storing person data by several Portfolio Initiatives. The result was that the specification was extensible to be a generic person; not specifically a terrorist person.

The use of the Person Data Specification was successful because it leveraged existing community work and because the Portfolio Initiatives that were affected by this specification collaborated and finalized the specification to be used in Quantum Leap-2.

Recommendation

The Person Data Specification should be published in the DoD Metadata XML registry.

4.2.5 Tactical (Track) Data Standard

The FY2004 Horizontal Fusion Portfolio included multiple track data consumers and providers. A tactical track data interface standard was developed to minimize the work required for a data consumer to obtain tracks from the multiple providers. The standard provides data definitions and web services operations for common track information such as accuracy and identification.

Observation and Analysis

The track data consumers and providers that were part of the FY2004 Horizontal Fusion Portfolio developed a common tactical data standard. Their approach was to adopt and incorporate a subset of pre-existing standards. The most significant problem they encountered in this approach was that existing standards remained specific to particular COIs. The lack of generality at the conceptual level limited their ability to apply these standards. When data items of interest lie at the bottom of a hierarchy, the entire hierarchy must be adopted to access the relevant item which increases network load with unnecessary empty data fields.



One of the standards initially incorporated into FY2004 was the Command and Control (C2) Information Exchange Data Model (C2IEDM), a relatively mature C2 data standard approved at the international level. As the Portfolio began to examine the lower, more granular levels of this standard, it became clear that the definitions were not applicable to many of the data providers. Schemas should be focused on generalizing existing and proposed standards at the conceptual level.

The standards that the Portfolio looked at were developed to suit specific applications, databases, etc. Standards need to be independent of applications, databases, etc. The specifications and standards should focus on the data.

Recommendations

Work within appropriate forums, the DoD XML Registry Namespace Managers, and C2IEDM Community to resolve differences between similar concepts to develop a community consensus on a consistent C2 and tactical ontology or taxonomy.

In the short-term, develop a common tactical taxonomy and schema for Horizontal Fusion track data.

Observation and Analysis

Regardless of specifications, guidance regarding standard methodologies to provide/consume the track data must be refined. In FY2004, track data Portfolio Initiatives used asynchronous mechanisms such as streaming and publish-subscribe to share information. The long-term requirement of the enterprise will evolve and become more robust based on the work done by Horizontal Fusion in FY2004.

Recommendation

Establish a community working group to define data exchange standards for sharing of near real-time data and to coordinate with the Organization for the Advancement of Structured Information Standards (OASIS) and the World Wide Web Consortium (W3C) on suitable web services technologies.

4.3 Development and Integration

Horizontal Fusion accomplished its development and integration activities on the NIPRNet and commercial provider networks in a Net-Centric fashion. Development in a Net-Centric environment is different from traditional program development and integration models, normally accomplished on closed networks by a small number of companies or organizations. Development and integration activities in a Net-Centric environment were complicated by 1) the hardware environment; 2) network connectivity; and 3) ports, protocol and firewall policies (site-specific and DoD) that affected both integration and deployment networks.

4.3.1 Hardware Environment

The Development and Integration environment was the set of servers which hosted the portal and core components of the Horizontal Fusion Portfolio for testing prior to production. The complex task of integrating the portlets and other code components was accomplished in this environment instead of on the production servers. This environment needs to expand so the unit testing for the Portfolio Initiatives occurs on one set of servers and the integration of the code and the associated configuration changes occur on another set.

Observation and Analysis

The development, test, and integration were conducted on the NIPRNet and commercial provider networks but the target deployment environment was the SIPRNet. Ideally, the development, test, and integration environments should replicate the target deployment environment as closely as possible. In FY2004, the services were hosted on hardware that differed between NIPRNet and SIPRNet.

The test and integration environment for Quantum Leap-2 was a single set of servers on NIPRNet and SIPRNet. This led to resource contention issues and reduced the amount of performance and reliability testing that is needed. Portfolio Initiatives providing portlets did not have access to a full environment during their development cycle, resulting in test and integration time being taken up with unit testing. The Portfolio determined that the development, test, and integration environment needs to have staging servers (portal and core services) for initial testing of fixes, then servers for integration and formal testing. These staging servers would increase the speed of integration, decouple development and test efforts, and support different levels of security functionality. Coordinating updates to the integration servers must be maintained throughout the test and integration process utilizing Net-Centric configuration management methodologies.

Some Portfolio Initiatives could not be fully tested on NIPRNet due to the lack of unclassified data or the lack of remote machines to serve this data. The data sets used on the NIPRNet need to be representative of the live data on the SIPRNet, including the users, their roles, and clearances. In other cases, the size and/or types of the data differed significantly between NIPRNet and SIPRNet. This led to unanticipated challenges during SIPRNet integration and testing.

Recommendations

The development, test, and integration environments should replicate the target deployment environment as closely as possible in terms of hardware connectivity.

Horizontal Fusion will set-up staging servers/reference implementations of the portal and core enterprise services to enable web services to be fully tested within the representative deployment environment.

Data sets, including the users, their roles, and clearances, used on the NIPRNet for test and integration must be representative of live data available on the SIPRNet.

4.3.2 Network Connectivity and Port/Firewall Restrictions

The nature of SOAs, including web service components, present many challenges to DoD standard operating procedures with regard to port/protocol and firewall connectivity. DoD currently operates in a mode where all connectivity be defined and controlled via site-to-site communications. This is to prevent unauthorized sites from gaining access.

Observation and Analysis

In a Net-Centric environment, a SOA would be able to “discover” services throughout the network without regard to server location. This is currently not possible with existing DoD guidelines for network connectivity. While implementing a SOA, the Horizontal Fusion Portfolio had numerous issues with exposing their services due to port exceptions and firewall access. Host sites of the services during the development and Quantum Leap-2 operations had firewalls preventing access to their internal networks, mostly by the use of Access Control Lists (ACLs), which corresponded to the specific Internet Protocol (IP) of a back-end service or client that wished to access the protected service. This was further complicated by the fact that policies governing firewalls on NIPRNet and SIPRNet are interpreted differently from site to site, resulting in some sites blocking all incoming service/user calls unless IP addresses/ports were staged in advance.

Accurate documentation for required ports would alleviate submitting requests for formal port exceptions. Existing Portfolio Initiatives and sites should also know their current network policies. Addressing SIPRNet connectivity issues early in the integration process would avoid many of the network problems encountered. These measures are a good first step to dealing with the challenges of an SOA implementation faces, but ultimately there are larger changes that must occur.

Recommendations

DoD must assess the current firewalls, ports, and protocol policies/mandates against a Net-Centric SOA concept and develop the policies/mandates that will support a secure SOA.



In addition, DoD should provide clarification and more comprehensive implementation guidance of the current policies/mandates. This will ensure consistency throughout DoD.

Observation and Analysis

Horizontal Fusion experienced problems with non-DoD sites (contractor, universities, DoS, etc.) that hosted services on the SIPRNet. These sites have severely restricted access to SIPRNet. Requesting and receiving site access to a single uniform resource locator (URL) realm (i.e. *Mars* Portal environment) using the DISA Disclosure Authorization (DA) process, resulted in only being able to access hardwired end-points and provided no ability to achieve Net-Centric functionality (users could get to the portal, but could not access any of the capabilities with out additional DAs).

Recommendation

Establish a working group with ASD/DISA/Defense Intelligence Agency (DIA) to build a Net-Centric SOA network security model and build a preliminary migration plan for security architecture.

Request DISA SIPRNet Approval Office assess the current DA process against the concept of a SOA and modify processes accordingly.

Observation and Analysis

Current DoD security culture and process are in conflict with the objectives of implementing an SOA. The very nature of an SOA implies no foreknowledge of who and where on the network a service will be accessed. Ultimately, ACLs as a mechanism for network protection are not easily scalable to the enterprise.

Recommendation

The network security model must be tied to the security service model of a SOA.

4.4 Net-Centric Enterprise Services (NCES) and Specifications

4.4.1 General

Under the auspices of the Net-Centric Enterprise Services Program, with DISA as the Executive Agent, DoD has directed the implementation of a global SOA to enhance data and systemic interoperability across the emerging GIG. Furthermore, ASD/NII and the Undersecretary of Defense for Intelligence have joint guidance for NCES to impact the resultant architectures on both SIPRNet and JWICS, planning for the eventual merge of all networked Department assets on the single GIG in the future.

Observation and Analysis

HORIZONTAL FUSION

Horizontal Fusion is implementing technologies in a leading edge SOA. Being in the forefront has allowed the Horizontal Fusion Portfolio to identify limitations with the current COTS/GOTS offerings that must be addressed before a widespread SOA can be fully recognized by the Department. For example, some commercial products have bugs that hinder integration and performance that results in memory leaks, thread leaks, differences in file descriptors, implementations of capabilities (e.g., replication) and lack of interoperability support among vendor products that implement the same standards. Most Portfolio vendor products did not support two-way SSL (a must for Net-Centric IA). The figure below illustrates the SOA at a high level that was implemented on the operational SIPRNet for Quantum Leap-2.

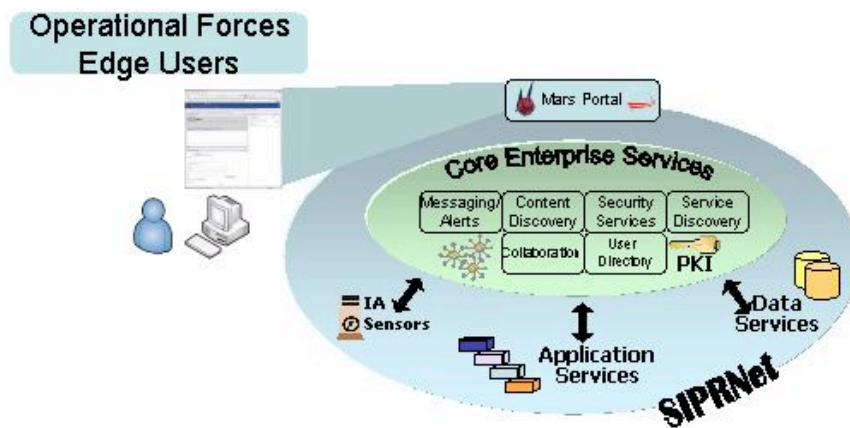


Figure 3 High Level SOA

Recommendation

Continue to investigate industry-accepted practices to solve SOA security challenges, including the use of Virtual Private Networks (VPNs) and secure tunneling between servers as cooperating technologies to the two-way SSL requirements.

Observation and Analysis



The core enterprise services will need to eventually support a heterogeneous global enterprise of application and data services. These services will have local policies, cross-domain considerations, and operational tempos unique to their domain. The concept of centralized application, service, and data warehouses will not support this hybrid enterprise. All core services will, therefore, need to be federated in such a manner that services, data, user tokens, global policies, and other artifacts of the SOA can be fielded, correctly discovered, and consumed. Also impacted by new SOA approaches is service reliability and availability. It is not adequate to cluster a service in a single location if the network connectivity to the cluster can be lost.

The core service standards that enable systemic and information interoperability require capability enhancements or fixes. These enhancements or fixes need to occur often and systematically (a three to six month release cycle), but should not effect the overall service specification. Service specification changes should occur less often due to the fact that any changes to these specifications have a huge impact across the entire SOA. The DoD Net-Centric community needs to investigate and develop an approach that will allow for specification changes while minimizing the impact to the operational SOA. Topics that need to be investigated include backwards compatibility, transition plans and ways to dynamically discover the service specification version needed to support individual web services during transition periods.

Recommendations

DISA must architect all Core Enterprise Services to support local and federated operations. Implementing the Core Enterprise Services in this manner will allow for truly distributed computing operations, monitoring, and failover.

Capability enhancements to the core components should be on a three- to six-month release cycle; however, specification changes should not occur on this cycle.

Horizontal Fusion, along with ASD-NII and DISA, must investigate guidelines for 1) supporting backward compatibility of APIs and formats; transitioning older specification elements with a proper support plan; and 3) maintaining services and discovering them dynamically through the service discovery mechanism.

Observation and Analysis

Web Services and Data Standards Working Groups need to prepare adequate documentation and software development kits (SDKs). The documentation must be updated in conjunction with changes to the software and/or specifications. Release notes, which indicate the reason(s) for the change, what was impacted by the change, and security and C&A effects must be provided for every iteration of the software and/or specification updates. Documentation on the service and data specifications must not specify tools, products, or environments. Having this documentation at the start of their development, the coders will have the necessary information for coding to the right standards, writing acceptable test cases, etc. Lack of this level of documentation in FY2004 resulted in code modifications during test and integration.

Recommendation

Each of the core services must have detailed documentation on the specifications, release notes for every drop, recipes for implementation including test cases, example implementation, and, if applicable, SDKs including source code.

Observation and Analysis

Since implementing an SOA is brand new to most developers, there needs to be regular hands-on developers conferences (seminars, technical exchange meetings, workshops). Each conference should have time allotted for detailed exchanges on a limited number of specifications. This will allow developers to work through the technical aspects, semantics, and implications of the specifications. It would allow developers the opportunity to share code and lessons learned. By also conducting these conferences on-line, the developers could link into their development environments and extract code where they have specific questions. This also allows developers who may be unable to travel to participate in the sessions.

Recommendation

NCES conduct developers conference sessions that will allow the developers to connect to the network, use the SDKs and sample implementations, and interface with the core service development and support staffs.

Observation and Analysis

All core configuration files, (i.e., WSDL and Service Mediation Descriptions (SMD)), need consistency and validity checking tools. These would allow integrators, testers, and system operators to confirm basic functionality and correctness without involving system developers when integrating new services or instantiations of existing services. This should be a precondition to embarking on the testing effort.

Recommendation

NCES should identify a suite of tools for checking the consistency and validity of core configuration files.

4.4.2 Security

For Quantum Leap-2, Horizontal Fusion utilized security services provided by both NCES and OED/JCDX. The NCES Security services provided the enterprise with a standard means of Certificate Validation (for both Personal Identification Certificates and Server Certificates) as well as a Policy Decision Service that enabled Role-Based Access to any registered enterprise service. OED/JCDX extended the NCES Security Services by providing Classification Policy Decision Service (cPDS) and a Clearance-Policy Decision Service called Security Adjudication Service (SAS). NCES Security Services, combined with OED/JCDX SAS, enabled the enterprise to set, apply, and maintain multiple classifications of data by ensuring that a user was exposed only to data consistent with their role and clearances. .

Observation and Analysis

For Quantum Leap-2, Horizontal Fusion demonstrated security services which allowed policy-based access to the core enterprise and various back-end services that made up the entirety of the Portfolio. These services included the NCES-provided Security Service and OED/JCDX-provided Classification Policy Decision Service (cPDS) and SAS. The NCES Security Services encompassed a number of functions, including a certificate validation service, LDAP query, and a role-based policy decision service. The OED/JCDX-provided security services provided clearance/classification policy decisions and adjudication of clearance dominance of a collection of appropriately labeled data elements. The implementation of the security services was perhaps the most challenging part of the FY2004 Horizontal Fusion effort.

There are currently multiple instantiations of the security services under different administrative controls with different back-end data stores (Policy, UDDI, and LDAP) that are not synchronized. Currently, a specific web service is configured to point to a specific instantiation of the security services which. With no federation of these services, they cannot function as a Net-Centric solution.

There were a number of observations made during FY2004 regarding the security services. First, security services must be federated and adapt to support both global and local policy decisions. It is imperative that individual operational areas retain control over their information and application access policies. A lack of federated policies also unnecessarily increases administrator burden and provides a single point of failure in each operationally deployed area.

Second, access to policies based only upon role and clearance attributes are insufficient to meet the needs of a networked force. While the current concept of “need to know” shifts to “need to share” in an SOA, there still will be requirements to potentially prevent (or at least direct)



access based on other attributes such as rank, operational component, location, etc., as well as support data aggregation privacy rights concerns.

Third, while the data model for classification and trigraphs are well defined by CAPCO and Federal Information Processing Standards (FIPS) guidance, data models for clearance and roles are not. Horizontal Fusion made some initial decisions regarding a sound clearance model and a workable hierarchical model for roles. A role model/schema is the set of acceptable roles a user can be assigned and the requirements a user must meet for having such roles. A proper role-schema is inherent to role-based access much the way Rank is inherent to military personnel. However, there are no common, DoD-wide role designations or definitions.

Fourth, the performance speed of the security services was an issue. There is significant latency involved when security information is not found. This can cause significant variances in response time for the web services. Additionally, the extensive digital signing of messages decreases performance because of the cryptographic operations required on both the client and the server. These operations make the server's scalability limited by processor speed rather than by input/output (I/O) performance.

Fifth, regarding distribution of the security services, Horizontal Fusion experimented with placing the security services at different locations. In particular, the cPDS was initially hosted in the Joint Intelligence Center, Pacific (JICPAC) while the other security services were hosted on the east coast. It was found that the latency introduced by the distance on the network for a core enterprise service induced too much of a performance hit to the portal and its back-end services. The cPDS instantiation was then co-located with the other security services. This increased performance of web service calls by as much as 70%. While an overall increase in bandwidth would mitigate some of the performance issues, there are still network architecture considerations to take into account. Latency is introduced with every switch, router, or media change (e.g., fiber to copper). A careful consideration of both bandwidth requirements and architecture distribution will be necessary to appropriately deploy an enterprise SOA.

Core services, especially highly utilized services like Security Services, can be the bottleneck of an operational enterprise. Federation (which allows utilization to be balanced over multiple instantiations) of these services will dramatically improve performance. In addition, single instances of these services would cripple the entire enterprise should that single instance fail; thus, there must exist multiple redundant services.

Quantum Leap-2 successfully demonstrated that appropriate metadata labeling of information is a valid and powerful tool for securing data. It demonstrated that data services could be quickly and easily federated into an SOA enterprise and consumed by both users and other services. While this is clearly one of the goals of Horizontal Fusion, it also highlights the potential for Data Inference and Aggregation concerns. Data inference is the deduction or reasoning of higher level classified information based on the availability of lower level, accessible information. Data aggregation occurs when a collection of accessible data takes on a higher security level than any of the elements in the aggregate. This is a concern for both protection of data from hostile forces as well as civil rights violations that are created when the



Department of Justice (DoJ), DoS, DoD, and the Department of Homeland Security (DHS) begin federating into this common data enterprise.

Recommendations

Core services, especially highly utilized services like Security Services, must be correctly architected and federated with multiple, redundant instances to support both performance and IA needs.

To reduce the latency associated with digital signature/encryption, evaluate the use of dedicated XML hardware acceleration and security devices for the cryptographic operations.

United States Joint Forces Command and Assistance Secretary of Defense/Network Integration and Infrastructure (ASD/NII) should sponsor a working group to establish hierarchical clearance and role schemas for the enterprise. These models must be extendable based on the requirements of the individual Services (i.e., United States Army, Air Force, Navy, and Marine) and Coalition partners.

The Policy Decision Service should be expanded to allow both enterprise level role-schema, as well as, locally applied role-schema to allow individual services the ability to govern policies regarding their own services.

NCES create an authoritative clearance acquisition service to allow any authorized service to acquire clearance information about a person.

ASD/NII should sponsor a working group to develop strategies to deal with issues of aggregation and inference.

4.4.3 Service Discovery

NCES Service Discovery Services (SDS) provide access to the UDDI Directory. UDDI can be considered the “Yellow Pages” of services within an enterprise; a listing and categorization of services. Service Discovery provides the ability to identify, locate, and retrieve services.

Observation and Analysis

As with any directory, UDDI is only useful when populated with relevant entries. Horizontal Fusion tried to use the NCES SDS for registering services into the directory. The tools for registration are the Management Console and Backend Registration Services. The Backend Service Discovery tools were not utilized by the Portfolio due to concerns with its security, management, and registration process. Instead, each service was registered manually through the Management Console.

Furthermore, these services were made discoverable via UDDI. To allow for maximum discoverability, services should be registered via a technical model. A technical Model (tModel), as defined by UDDI, is a structure containing an abstract and reusable specification.



It has a unique key (generated by a UDDI server), a name, a description, and a URL. It can be used to form a taxonomy for the classification of services. Horizontal Fusion implemented a standard tModel for the track service providers, which was used to map one service implementation to the C2Visualization standard. However, tModel schemas were not developed for the majority of the other services that existed in Horizontal Fusion. Because there is not current tModel infrastructure to leverage within the DoD, a new infrastructure must be built to register COI-specific services into UDDI.

The immaturity of the NCES SDS hindered service discovery for Quantum Leap-2. Service providers lacked the ability to manage their own services within UDDI. In addition, the more mature standards like WSDL and UDDI specifications were not adhered to by the NCES SDS and its tools, further complicating any enterprise level service discovery.

Recommendation

The service taxonomy and definitions need to be standardized across DoD and the Federal Government.

To support an enterprise federated application registry, the NCES Program must engage the DoD community to define the tModel infrastructure.

NCES incorporate more mature standards like WSDL and UDDI specifications into the NCES SDS.

Observation and Analysis

Currently, for a service to be protected by the security services, it must first be registered through the NCES SDS GUI. This unnecessarily complicates the architecture and makes the management of services impractical to scale. While any steps added by the decoupling of the SDS from security services may appear to be a burden, over the long-term, service registry management will flow more smoothly.

Ultimately, the Horizontal Fusion Portfolio's Quantum Leap-2 proved that a service registry is an integral part of an SOA. However, commercial technologies, other than UDDI, may ultimately be used to provide this capability. Using a government abstraction layer such as the NCES SDS complicates the architecture and makes it costly to integrate with/leverage off the shelf commercial registries/capabilities. The time required to code and recode an the NCES SDS makes it impractical to quickly adapt and implement newer technologies (e.g., federation, dynamic registration).

Recommendation

The NCES SDS should be retired in favor of a purely standards-based registry infrastructure.

4.4.4 Content Discovery

Horizontal Fusion defined NCES Content Discovery specification on behalf of DISA and then provided an implementation of the enterprise service. The Content Discovery service enabled warfighters, decision-makers, and support personnel access to all relevant knowledge from across the entire spectrum of data sources. The query response was then presented to the user in an immediately understandable manner.

Observation and Analysis

Content Discovery, known as Federated Search, is a powerful demonstration of the SOA. Federated Search provides access to many heterogeneous and geographically dispersed types of data.

Recommendation

As the SOA grows, equal emphasis must be put on increasing the number of registered data providers as well as enhancing the current Content Discovery capabilities.

Observation and Analysis

Content Discovery is accomplished by query routing based on the taxonomy or ontology. During the development and integration period, Initiatives must spend the time to verify they have properly registered their data source(s) into the taxonomy. Development and Integration testing will allow the Initiatives/functional users to determine if the proper data is being returned from the enterprise query. This process requires fine tuning and participation on the part of the data providers.

Horizontal Fusion is implementing a data provider quality assessment plan. This will allow providers to verify their capabilities, both from a technical (specification compliance) and a functional (quality and applicability of results) perspective. HF will use this assessment to determine which data providers are of sufficient quality to be used in an operational environment.

Quantum Leap-2 helped identify a new requirement that would greatly enhance the Content Discovery core service implementation. A query aggregator capability would both provide the user with a very useful tool as well as help reduce stress on back-end data providers. The query aggregator would allow for a second query to run against a first set of returned results. For example, if a user received 300 possible matches to a query, the query aggregator would allow a second query to run just against that set of 300 returns. This allows the user to further refine the first query without starting over and reduces the number of data providers and amount of data that needs to be searched on the second query.

Recommendations



Content Discovery data providers need to verify that they have properly registered their data sources into the taxonomy and must enact a level of quality control to ensure the best data results are returned to user queries.

Content Discovery should be further enhanced with additional capabilities, such as a query aggregator.

Observation and Analysis

The Federated Search must handle geospatial queries for a number of geospatial Horizontal Fusion data providers. The DDMS schema, which is incorporated into the Content Discovery Specification, provides very little support for geospatial information. NGA is now collaborating with DDMS to augment the geospatial tags.

Recommendation

Request the DDMS Focus Group and NGA continue to work closely together to include/extend geospatial aspects within the specification and publish the results to the DoD Metadata XML Registry while also working with the DoD Namespace Manager's Forum for the overarching COI schema.

4.4.5 Person Discovery

The Person Discovery Service provides for the dynamic discovery and manipulation of person data. Persons are treated as data objects, thereby allowing seamless integration with the other components of the NCES Discovery Services. The Person Discovery Service is integrated with the NCES Security Services, Content Discovery, Collaboration, and the Horizontal Fusion "Find the Expert" capability.

Observation and Analysis

The Person Discovery Services are integrated with the DISA GDS. GDS contains identification data about all users who have received DoD PKI certificates. GDS is implemented in a Netscape LDAP directory. The core LDAP has the schema defined by the GDS. This core schema did not support all the requirements for DAC+ or the Person Discovery capability. Horizontal Fusion, in coordination with the DISA GDS program, extended the schema to include clearances, roles, phone numbers, expertise descriptions, email addresses, and areas of expertise.

This extended LDAP directory was initially loaded with data exported from the GDS directory and subsequently updated via an automatic process as changes occurred in GDS. This process, called Live Update, is a DISA GOTS product that pushes data changes to remote LDAP servers.



The Person Discovery Service insulates all person discovery service consumers (including the *Mars* portal) from LDAP connectivity issues and schema changes. The current Person Discovery Specification supports the needs of all *Mars* portal expert visualization portlets, including expert registration and expert search.

The Person Discovery service provides access to the core LDAP and the Horizontal Fusion extensions. Consumers of person data can access the extended LDAP using direct access, the Person Discovery service, or a helper class called the PortalRBACBean. Of these methods, the PortalRBACBean, was by far the most widely used because it provided simple access and insulation from LDAP schema modifications. Web services that operated on the .NET operating environment could not use the PortalRBACBean (due to the fact that the PortalRBACBean only operated within an Axis environment) and generally used direct LDAP access.

There was inconsistency on the method by which users were identified in the SOAP message headers. Some Portfolio Initiatives provided the PKI Common Name (C/N) while other Portfolio Initiatives provided the PKI Distinguished Name (D/N). Both the C/N and the D/N are text strings, so this inconsistency was not readily apparent at the API level.

Recommendations

In the Developer's guidance, provide direction on how Portfolio Initiatives should access the LDAP as well as asserting D/N in the SOAP message header.

The PortalRbacBean concept should be expanded to support other operating environments (i.e., .NET) and should be appropriately documented with the same rigor as the core services.

4.4.6 Mediation Messaging/Alerts

The Messaging Service provides a general purpose publish/subscribe-based event notification capability. Consumers subscribe for one or more topics, or subjects of interest. Producers publish messages to relevant topics and the Messaging Service determines which consumers should receive the message and reliably delivers the message to those consumers. The Messaging Service replaces multiple custom publish/subscribe interfaces allowing interoperability between existing data providers. The goal of the Messaging Service is to provide a distributed, federated architecture consisting of multiple brokers interconnected via an overly network. The Messaging Service provides this capability via a native Java Messaging Service (JMS) interface (a commercial application) and a Web Service interface based on the proposed WS-Eventing specification (a commercial specification). The DIA Virtual Knowledge Base alerts system leverages the messaging service and provides additional content-based categorization of published messages and profile-based subscriptions for messages.

Observation and Analysis



For Quantum Leap-2, Horizontal Fusion fielded a JMS-based messaging capability to support the publish/subscribe requirements of the enterprise. This capability provided "channels" which, once subscribed to, would deliver data to the consumer. A "channel" allows messages with similar topics and/or subjects to be grouped. The benefits of the "channels" are that users do not need to know specific information about a message (i.e. publisher, date published, title, etc.) in order to receive those messages, and the message provider does not need to keep track of the entire community that is interested in receiving new messages. For example, a user can subscribe to a generic channel such as "Russian Air Force" and receive both generic and detailed messages concerning the Russian Air Force from different data providers who report on the Russian Air Force. As new data providers become available, they can provide information on the Russian Air Force without having to know all the specific users who are interested in receiving their messages.

In general, the Department's Mediation Messaging specifications and guidance are immature and only partially published. This complicated the development of capabilities which could use the messaging capability due to a lack of understanding of how to correctly build to the interface (i.e., when to use a channel, channel administration, how to bind to a channel, etc.). Quantum Leap-2 helped identify several new requirements including an enhanced registration, explicit support for accessing historical messages within a channel, a categorization service to allow automated messages to be sent to multiple channels, and links into the Mediation Services to transform the format of a message.

Many Initiatives were late realizing that the messaging specification provided a framework for communication among members of any COI and did not force the members to use specific message formats. The definition of the message format is reliant on any specific community. This led to confusion about who produced the specifications for the messages for the various COIs. For example, in Quantum Leap-2 there were multiple COIs including Alerts and Person Load. The Collateral Space Initiative defined the Alerts Message specification in FY2003. The Alerts specification is used to transfer alerts over the Messaging Service. To support sharing of person information across the messaging service, the NORA Initiative created the Person Load message specification. The person load specification defined a message that took in an array of person objects, as defined by the person specification. The Non-Obvious Relationship Awareness (NORA) Initiative created and implemented the web service to receive person information. The Messaging Service is a powerful capability, but is a difficult service to truly comprehend. In order to maximize the potential of the service, data providers need to be educated on the benefits of using the capabilities (such as sending alerts and passing person data) within the service.

There were also some technical issues with both the Native JMS providers and the Web Services specifications. Native JMS vendors do not support two-way SSL adequately. In addition, there is no clear way to integrate all the NCES security services (which are designed to support web services) into native JMS provider capabilities. The Messaging service has security considerations which are different from the security considerations of conventional direct-connect web services. For example, by design, the messaging service acts as a mediator between the producer and the variable set of consumers. As a result, the producer does not

know the set of consumers to which the message is delivered. This differs from a trusted communications where the producer always knows the identity of the recipient. The DoD Net-Centric community needs to establish tiger teams to address how to implement security requirements needed for Information Assurance using commercial applications that do not need to address these more stringent requirements within the commercial sector.

Recommendation

Extend the Mediation Messaging specification to fully support Alerts functionality.

Since the Person Load message was defined and used by only two of the Portfolio Initiatives, there is a need for other providers of person objects to review, accept, and refine the message specification.

Mediation/Messaging service documentation needs to include guidance on when and how publishers should use the Messaging capabilities.

COI's must determine their message formats.

To ensure the Net-Centric community handles the unique requirements needed to meet DoD Information Assurance, Horizontal Fusion suggests the NCES Security Services working group establish a tiger team to develop a CONOPs addressing the integration shortfalls between security services and the messaging service.

4.4.7 Collaboration

While the SOA naturally fosters collaboration between services and users, it has specifically identified "collaboration services" as a set of capabilities to enable users to share and simultaneously work on content or find and directly communicate with each other. This included services such as presence awareness, text-based chat, video-teleconferencing, and shared whiteboarding.

Observation and Analysis

For Quantum Leap-2, Horizontal Fusion demonstrated two main collaboration services from within two Portfolio Initiatives: Trusted Wisdom and Knowledge Management and Collaboration in a Net-Centric Environment (KMINCE). KMINCE provided a Hyperwave-based capability, which provided textual-chat, presence awareness, network audio and video teleconferencing, white-boarding, and application sharing. Trusted Wisdom provided a Jabber-based textual chat capability. Through a Jabber-bridge, provided by KMINCE, users of both systems were able to communicate with each other using textual chat. In other words, because both services followed a commercial collaboration standard, different users were able to use the collaboration tool of their choice and still communicate with each other without having to establish a special point-to-point interface. This is the true definition of interoperability.



In addition, a web service interface was specified and implemented by KMINCE to allow integration of the tool in an SOA. The web service interface allows querying online status of users, launching collaboration sessions, and access to other collaboration functions. For the Expert Search functionality, this web service interface was successfully used so that users could immediately start collaboration sessions with any experts found.

For collaboration, communication across domain boundaries (especially Clearance/Releasability) is complex. Establishing and maintaining collaboration sessions with users (including adding/removing users) from various clearances and countries are non-trivial. The problem in this set of services is similar to the data inference/aggregation problem, except further complicated by the fact that it deals with direct human-to-human interaction. By integrating with the cPDS, the KMINCE solution demonstrated how collaboration sessions between users with different clearances/from different countries can be established.

As with the other services, without a standard set of specifications for each collaborative technology area, there will not be interoperability of toolsets. While consolidating to a single toolset is not the answer, a particular toolset may contain certain functions that might better support a specific set of operational requirements. However, Quantum Leap-2 proved that different vendors' tools can be interoperable. More complicated functions of collaboration (e.g., video teleconferencing, application sharing, etc.) require a significant amount of bandwidth.

Recommendation

Real-time intelligent tagging services must be developed to label and process audible and text information for cross-domain information exchange/releasability.

Until then, user training with respect to collaboration "rules of engagement" must be developed to avoid security violations.

A further analysis of data compression and more efficient formats must be conducted for bandwidth intensive functions, such as video conferencing and application sharing.

ASD/NII and DISA must provide guidance on the set of open commercial standards-based specifications for collaboration as part of the announcement of the next generation of the Defense Collaborative Tool Suite to promote multiple tool interoperability.

4.4.8 Enterprise Service Management (ESM)

The ESM core service focuses on monitoring the communications between services and portrays a picture of enterprise service activity and health. Due to the lack of commercially available specification/standards-based monitoring tools for web services, Horizontal Fusion defined a specification.

Observation and Analysis

As Net-Centricity moves into full operation, the need for monitoring capabilities is becoming increasingly evident. The monitoring of large enterprise networks is often referred to ESM. The current technology limitations of ESM COTS products related to secure, web services-based networks become very evident over the past year. An essential element of Net-Centricity is the movement of information, not just the connectivity of systems. A common approach to ESM is a "heart beat" or a "ping" type approach. This basically uses tools to assure front-end hardware and basic software systems are alive. The difficulty in an SOA is that a web service being "up" does not actually mean that much to the final performance of the architecture. A web service can be "up" but the back end systems that feed that service may not be providing the critical information that the warfighter needs.

During FY2004, a standards-based approach to monitoring information flow was developed and demonstrated. This approach tackled two major issues, 1) how to characterize information flow content and 2) how to do so in a secure environment. The approach used a handler deployed in the web services to be able to determine not only the status of the web service, but to characterize and display in real time the information moving from the service and onto the network. As the SOA is moved into an operational status, this capability will be essential to knowing the overall health of the information flow across the net.

In addition, the current availability of commercial monitoring tools on the market does not meet the basic needs of SOA in the DoD. In particular, the monitoring of information content in a secure environment is not a focus of most commercial vendors. A standards approach to defining the handler, which extracts information from the services, needs to be followed to take advantage of this emerging technology.

The Visual Enterprise Monitoring (VEM) Portfolio Initiative implemented an ESM handler in FY2004. The handler approach differs from commercial approaches in that it monitors actual information flow and its content while commercial tools monitor service availability. This inherently leads to an incomplete picture of the health of the enterprise. This led to supplanting the ESM capability with tools that tested the availability of the server; however, it did not have the ability to indicate the availability of a service. Quantum Leap-2 helped identify a new requirement—extend the service to include information flow. It would be beneficial to derive a specification for a service to respond to availability queries, similar to "pings," in addition to the handler. Core services should be monitored on a real-time basis and work with Federated Services to reroute if the primary dies. Another requirement is to report and log a system with an "alive" or "dead" status, along with service load data, and should be monitored as well. The combination of the health status and handler approach would provide the ability to monitor both "Who is Out There" and "What They Are Doing", a much more complete ESM picture than is currently available.

Recommendation



As NCES matures the ESM specification, they should include the fact that any enterprise monitoring capability must be able to assess the availability of hardware, software, and the network as well as what content is going where.

The specification defined by Horizontal Fusion should be reviewed and refined through the NCES community process.

5 SUMMARY

The work of the Horizontal Fusion Portfolio has expanded the capabilities of the Secret Internet Protocol Router Network (SIPRNet) by establishing a services-oriented architecture (SOA) that mirrors the business equivalent of an internet service provider. The ability for users of the Portfolio's SOA to pull mission-critical data has a direct, positive impact on "speed of command" at all levels. Horizontal Fusion has established a new paradigm for combat forces managing data in a hierarchy. Troops at all levels now have the capacity to be both a data provider and data consumer and can "pull" mission-critical information from the databases of the Department of Defense (DoD) and other U.S. agencies as mission and priorities change in an asymmetrical environment. Horizontal Fusion has not only made an impact on the decision support process at the Joint Task Force (JTF) level; it has provided near-real time access to the operational support data that forces require for combat execution.

The Horizontal Fusion establishment of a SIPRNet SOA has built a solid framework for cost effective interoperability among existing DoD programs of record. There is no need to build an SOA "from scratch". Existing Programs of Record can modify their operational baselines to "attach" to an information sharing environment maximizing the Department's legacy investments which increases our return on current investment. New acquisitions must be built to the evolving standards and specifications. Horizontal Fusion has proved that this evolutionary approach is not only implementable but cost effective and extremely timely. In FY2004 over 30 Portfolio Initiatives produced the necessary front ends and passed through test and integration in 5 months. All Portfolio members could post their information to the Collateral Space in accordance with established standards. Users could define their information needs, pull appropriate information from a variety of sources, assess the information for value, and post additional information. Communities of Interest (COIs) dispersed across the globe, but connected to the Collateral Space through the SIPRNet, could immediately share data.

The Horizontal Fusion Portfolio has successfully addressed the five critical GIG architectural tenets:

- **Only handle information once.** Collecting information and entering data multiple times introduces errors in the data, is costly, and adversely affects efficiency in both combat and business operations. The Horizontal Fusion SOA allows data to be quickly exposed within the Portfolio, minimizing the time and effort dedicated to data collection and dissemination.
- **Post before processing.** The Horizontal Fusion SOA can accommodate the task, post, process and use model for information sharing. As data becomes available, it can be immediately posted to the Collateral Space and accessed by all members of the Portfolio. The identical data and information that provides the basis for finished intelligence products can be expeditiously utilized by the warfighter and other COIs. This will lead to an improved command decision-making process.
- **Users will pull data** as needed instead of having massive amounts of information pushed to them regularly—some of which may be irrelevant to their current mission. A key tenet

HORIZONTAL FUSION

of Net-Centric warfare is that the consumers of information know best what they require of available data sources and must have the ability to pull that data when they need it as their circumstances and mission requirements constantly shift. Further, the Collateral Space (Quantum Leap-2 demonstration version) provides access to information across information domains.

- **Sense-making tools and Collaboration technologies** have been employed within the Collateral Space to assist users in effective utilization making sense of the data they pulled. For example, subject matter experts from diverse units or organizations can now come together as COIs to make sense out of special situations. The ability to pull expertise from within a unit, as well as from across the Collateral Space, is a value-added feature of the Horizontal Fusion Portfolio environment. Tools that currently do not exist within the warfighters operational baselines (basic language translation, complex pattern recognition, large data set visualization, etc.) are now available to all users to access the information sharing environment.
- **A reliable network is key.** Diverse and robust information pathways must be in place to ensure reliability. The preliminary work on the discretionary/mandatory access controls, along with cross-domain information exchange, has been established on the operational SIPRNet at the Interim Authority to Test (IATT) level.

The pace of advancing technology requires that a move from an approach that is based upon application standards to one based on data standards is a must. The comprehensive impact of the Horizontal Fusion Portfolio's SOA and the development of standards has been the key to giving Collateral Space users an opportunity to use the applications that make sense to them while maintaining the ability to exchange data. The Collateral Space focuses on support to peer-to-peer relationships and information exchanges that transcend individual systems and organizations.

Outlook for FY2005

In FY2004, Horizontal Fusion demonstrated that Net-Centric transformation is not only feasible but the necessity for Net-Centricity to become an integral part of battle operations. In FY2005, the Horizontal Fusion Portfolio will accelerate delivery of the Net-Centric environment and capabilities demonstrated in Quantum Leap-2 to an operational setting. In addition to "operationalizing" this Net-Centric environment, Horizontal Fusion will continue to enhance its baselined SOA by continuing to develop and deliver core enterprise services, as necessary.

The FY2005 Horizontal Fusion Portfolio will capitalize on its current Portfolio investments by retaining as many Portfolio members as possible, however, continued participation for each of the FY2004 Portfolio members is contingent upon their past performance. Horizontal Fusion also intends to incorporate two existing local SOA networks into the FY2005 Portfolio—the U.S. Army's XVIII Airborne Corps FusionNet and the DoD's Explosive Ordinance Disposal (EOD) community's JEODNet. Both will be incorporated into the Collateral Space and will have access to the Horizontal Fusion SOA infrastructure and tools. It is anticipated that both of these units will employ the Horizontal Fusion SOA in an operational environment, thereby



providing a true assessment of the effectiveness of Horizontal Fusion and its SOA in support of operations.

A second goal for Horizontal Fusion in FY2005 is to continue developing and implementing key areas of the SOA, particularly as it relates to Information Assurance. These key Information Assurance areas include the certification and accreditation process and cross-domain information exchange between multiple networks or domains. Horizontal Fusion will use the accomplishments of FY2004 as a stepping stone to further the needs of Coalition information sharing capabilities.

A third goal of Horizontal Fusion in FY2005 will be to incorporate as many new Portfolio Initiatives as possible into the Portfolio. New Portfolio members will be selected based on their potential to substantially address the warfighter's needs and to complement the Portfolio's existing capabilities.



6 INITIATIVE DETAILS

<i>NAME</i>	<i>SERVICES PROVIDED</i>	<i>SPONSOR</i>
Basic Language Translation Services (BLTS)	Provides language translation services (printed documents and speech) and makes available information via Warrior's Edge.	United States Army G2, Army Research Laboratory (ARL)
Coalition Shared Intelligence Networked Environment (COSINE)	Combines analysis/production-sharing and cross-coalition information management with a secure network structure. Intelligence exchange, content-based information security, and release management capabilities will allow individual coalition domains to quickly connect to secure coalition command and control (C2) and intelligence systems in a near real-time secure manner.	North Atlantic Treaty Organization (NATO) Consultation, Command, and Control Agency (NC3A)
Collateral Space	Is a globally accessible, shared information space providing improved and increased visibility to intelligence and operations information through a standards-based interoperability framework.	Defense Intelligence Agency (DIA)
Content Staging	Provides discovery, indexing, retrieval, storage, and publish-subscribe services (smart pull) of information products critical to the warfighter in intuitive, Web-browser form. Currently operational at 30 locations including Operation Enduring Freedom, Operation Iraqi Freedom, and Liberia.	Defense Information Systems Agency (DISA)

HORIZONTAL FUSION

<i>NAME</i>	<i>SERVICES PROVIDED</i>	<i>SPONSOR</i>
Cooperative Engagement Capability (CEC)	Provides access to the CEC sensor network's real time air track picture and makes it accessible to a variety of clients. Intelligent pull allows tailoring of the data requested for either current or historical track data and underlying measurement data, or streaming data to constantly update track movements.	United States Navy
Defense Strategic Integrated Decision Environment (D-SIDE)	Provides a secure, classified course of action (COA) decision-making capability providing tools, processes, and procedures to define, share, refine, de-conflict, and merge proposed COAs across combatant commands, for presentation of an integrated set of options for approval by national leadership.	United States Strategic Command (USSTRATCOM)
Department of State: Net-Centric Diplomacy	Enhances the warfighter, mission planner, and combatant commander's ability to gain situation understanding about adversaries and their operating environment by providing a full range of diplomatic reporting from worldwide posts.	Department of State (DoS)
Environment Visualization (EVIS)	Produces forecasted weather effects on tactical missions and makes these available and advertised. This enables a user to access high resolution, mission-tailored weather effects summaries and related map overlays within their tactical decision-making cycle.	Naval Research Laboratory (NRL)
Extensible Tactical C4I Framework (XTCF)	Provides an architecture that will rapidly add new services and get new content providers and consumers quickly into the Collateral Space in a dynamic battlespace by utilizing an open, extensible plug-and-play architecture that will transform C2 data management services.	Office of Naval Research (ONR)

HORIZONTAL FUSION

<i>NAME</i>	<i>SERVICES PROVIDED</i>	<i>SPONSOR</i>
FusionNet	Provides leaders, staff, and individual soldiers at the company through corps echelons with an integrated application suite to manage their units, plan and execute deployments and tactical operations, sustain their forces, and report operational, intelligence, and logistics information through easy-to-use, network-friendly smart client and web-based user interfaces. This bottom-up data is exposed to the Collateral Space to give decision makers timely and accurate “ground truth” information on both the friendly and enemy situations.	United States Army, XVIII Airborne Corps
Global Net-Centric Surveillance and Targeting (GNCST)	Distributes target reports to tactical users in tactically relevant time. This is a developing capability to demonstrate model-based fusion of upstream data from multiple intelligence sources to detect, locate, and identify time-critical targets and targets of national interest.	National Geospatial-Intelligence Agency (NGA)
Integration of Non-Traditional Information Sources (INTIS)	Uses non-traditional sensors, (F/A-18 Hornet, AH-64 Apache), to provide secure, rapid delivery of hostile surface-to-air missile and anti-aircraft electronic intelligence to the warfighter and the intelligence community.	Office of the Secretary of Defense/Distributed Common Ground System (OSD/DCGS)
Open-Source Information System (OSIS) Evolutionary Development (OED)/ Joint Cross Domain eXchange (JCDX)	Supports the customers of the U.S. and partner Joint Intelligence Centers with information tailored to their clearance level, area of interest, and need to know. This is the only operational command, control, communications, computers, and intelligence system trusted to provide a multi-level secure capability.	United States Navy
Joint Surveillance Target	Enables tracking more targets with greater accuracy by means of a	Electronic Systems

HORIZONTAL FUSION

<i>NAME</i>	<i>SERVICES PROVIDED</i>	<i>SPONSOR</i>
Attack Radar System (JSTARS)/Affordable Moving Surface Target Engagement (AMSTE)	sophisticated moving-object tracking capability. JSTARS/AMSTE can push these tracks to a ground station, with the ground station converting both the moving target indicator reports and tracks into an eXtensible Markup Language (XML) message for publication.	Command/JSTARS
Knowledge Management in a Net-Centric Environment (KMINCE)	Provides a web-accessible, multilingual environment where analysts/users can collaborate, build, and post intelligence products based on the National Ground Intelligence Center's (NGIC's) digital production program.	NGIC
Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition (MAJIIC)	Enhances U.S. joint and coalition intelligence, surveillance, and reconnaissance (ISR) data interoperability. Facilitates information sharing via the development, testing, and implementation of data standards, XML schemas, and leading edge Web-based enterprise services. MAJIIC will "post- before processing" to collateral space, providing discovery and smart pull.	United States Joint Forces Command (USJFCOM)
Naval Research Lab (NRL) Sensor Node	Provides an airborne node for target location and detection to support ground troops and joint strike forces directly by posting "sensor products" (e.g., imagery, data, reports) and alerts for immediate use in operational planning.	NRL
Net-Centric Geospatial-Intelligence Services (NGS)	Provides warfighters and senior policymakers with access to geospatial intelligence (GEOINT) and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on Earth.	NGA
Non-Obvious Relationship Awareness	Discovers relationships among people and organizations to answer the question, "Who knows whom?" Accessed by the warfighter through	SPAWAR Systems Center, Charleston

HORIZONTAL FUSION

<i>NAME</i>	<i>SERVICES PROVIDED</i>	<i>SPONSOR</i>
(NORA)	the <i>Mars</i> Portal.	
Project Garnet	Provides access to National Security Agency (NSA) analysts via virtual private networking to thin client computers. This enables multiple security domain connections with the same infrastructure and rapid deployment of networks without installing new cable plants or desktops.	NSA
Secure Mobile Networks	Provides the warfighter with secure, robust voice and data mobile wireless communication networks that enable collaboration even in highly dynamic, unpredictable environments. These are intelligent, resilient, and self-configuring networks that allow access to global assets in the field even when direct links with reachback communications are not available.	ARL
Tearline Reporting (TLR)	Identifies and extracts the sanitized section (tearline) of intelligence reports and posts (or disseminates) them, with near real-time posting in a database format that is exploitable by federated search and other Web services.	United States Army Information Security Command (USAINSCOM)
Test and Evaluation	Provides the Test and Evaluation instantiation of the Collateral Space for use during testing and integration. It is used to assess and evaluate new technologies to enhance the engineering environment and provide	SPAWAR Systems Center, Charleston

HORIZONTAL FUSION

<i>NAME</i>	<i>SERVICES PROVIDED</i>	<i>SPONSOR</i>
	a developers “sandbox” for testing and integration of products before introduction into the operational Collateral Space. Assists Portfolio Initiatives and Partners as necessary to transition their programs into the operational Net-Centric environment. Provides direction, oversight, and execution of the testing and verification of the Horizontal Fusion Portfolio enterprise services.	
Trusted Wisdom	Provides secure, mobile, real-time posting of reporting from field collectors. Information is tagged, enabling communities of interest to host rapid analysis and fusion of field collector reporting and technical collection data. Allows field collectors, analysts, and warfighters to interact and rapidly develop actionable intelligence.	DIA
Trusted Workstation (TWS)	Provides intelligence analysts and operational warfighters with on-demand simultaneous access to common and mission-critical desktop applications running at multiple security domains from a single ultra-thin-client workstation.	United States Pacific Command (USPACOM)
Ubiquitous Automated Information Manager (U-AIM)	Enables the aiming of external information to automatically discover, access, associate, and prioritize intelligence and information products. Focuses and allocates resources on high priority information needs. This allows the warfighter to formulate target or event nomination and receive alerts, all tailored to the role and mission.	Pennsylvania State University/Applied Research Laboratory
Visual Enterprise Monitoring (VEM)	Provides a “window to the information flow” within a network to increase commanders’ and decision-makers’ overall situational awareness.	Ogden Air Logistic Command

HORIZONTAL FUSION

<i>NAME</i>	<i>SERVICES PROVIDED</i>	<i>SPONSOR</i>
Visualization/Information Dominance (V/ID)	Bridges traditionally separate analytic processes, including data preparation and exploitation, and Web-enables it through data extraction, analysis, and tagging via the commercial ClearForest ClearTags entity extractor. Visualization capability is enhanced/enabled using the commercial Starlight toolkit.	USAINSCOM
Warrior's Edge	Represents a dynamic, ad hoc, networked local sensing environment. Comprised of soldiers, robotic sensors, and unattended sensors. Each provides a user-tailored perspective of the combat situation to the warfighter during changing conditions to maximize mission success.	United States Army G2/ARL

7 ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
AIM	AOL Instant Messenger
AMSTE	Affordable Moving Surface Target Engagement
API	Application Program Interface
ARL	Army Research Laboratory
ASD/NII	Assistant Secretary of Defense for Networks and Information Integration
BLTS	Basic Language Translation Services
C&A	Certification and Accreditation
C/N	PKI Common Name
C2	Command and Control
C2IEDM	Command and Control Information Exchange Data Model
CA	Certificate Authority
CAC	Common Access Card
CAPCO	Controlled Access Program Coordination Office
CEC	Cooperative Engagement Capability
CIO	Chief Information Officer
COA	Course of Action
COCOM	Combatant Command

COI	Community of Interest
CONOPs	Concept of Operations
COSINE	Coalition Shared Intelligence Networked Environment
COTS	Commercial-Off-The-Shelf
cPDS	Classification Policy Decision
CRI	Certificate Registration Instructions
CRL	Certificate Revocation List
D/N	PKI Distinguished Name
DA	Disclosure Authorization
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DAC+	Discretionary Access Control-Plus
DARPA	Defense Advanced Research Projects Agency
DCID	Director of Central Intelligence Directive
DDMS	Defense Discovery Metadata Specification
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DoDD	Department of Defense Directive
DoJ	Department of Justice

DoS	Department of State
D-SIDE	Defense Strategic Integrated Decision Environment
DSWAG	Defense Information Systems Network (DISN) Security Accreditation Working Group
EIE	Enterprise Information Environment
EIW	Enterprise Integration Workshop
ERB	Engineering Review Board
ESM	Enterprise Service Management
EVIS	Environment Visualization
FFP	Firm Fixed Price
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
GDS	Global Directory Services
GEOINT	Geospatial-Intelligence
GIG	Global Information Grid
GIG-BE	Global Information Grid Bandwidth Expansion
GNCST	Global Net-Centric Surveillance and Targeting
GOTS	Government-off-the-shelf
GUI	Graphical User Interface

I/O	Input/Output
IA	Information Assurance
IATO	Interim Authority to Operate
IATT	Interim Authority To Test
ICMWG	Intelligence Community Metadata Working Group
IFIS	Intelligent Federated Index Search
IMS	Integrated Master Schedule
INTIS	Integration of Non-Traditional Information Sources
IP	Internet Protocol
ISM	Information Security Marking
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
IWG	Integration Working Group
JCS	Joint Chiefs of Staff
JEOD	Joint Explosive Ordinance Disposal
JICPAC	Joint Intelligence Center, Pacific
JITC	Joint Interoperability Test Command
JMS	Java Messaging Service
JRE	Java Runtime Environment
JSR-168	Java Specification Request Number 168
JSTARS	Joint Surveillance Target Attack Radar System
JTF	Joint Task Force

JTRS	Joint Tactical Radio System
JWICS	Joint Worldwide Intelligence Communications System
KMINCE	Knowledge Management and Collaboration in a Net-Centric Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Control
LRA	Local Registration Authority
MAC	Mandatory Access Control
MAJIC	Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition
MIPR	Military Interdepartmental Purchase Request
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation, Command, and Control Agency
NCES	Net-Centric Enterprise Services
NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NGS	Net-Centric Geospatial Intelligence Services
NIPRNet	Non-Secure Internet Protocol Router Network
NORA	Non-Obvious Relationship Awareness
NRL	Naval Research Laboratory

NSA

OASIS	Organization for the Advancement of Structured Information Standards – drives the development, convergence, and adoption of e-business standards. OASIS is a not-for-profit, international consortium.
OED/JCDX	Open-Source Information System (OSIS) Evolutionary Development/Joint Cross-Domain Exchange
ONR	Office of Naval Research
OSD/DCGS	Office of the Secretary of Defense/Distributed Common Ground System
OSIS	Open-Source Information Systems
PKI	Public Key Infrastructure
PL	Protection Level
POR	Program of Record
RA	Risk Assessment
RadAC	Risk Adaptive Access Control
RBAC	Role-Based Access Control
ROM	Rough Order of Magnitude
RWS	Registration Web Service
SAML	Security Assertion Markup Language
SAS	Security Adjudication Services
SCAO	SIPRNet Connection Approval Office

SDK	Software Development Kit
SDS	Service Discovery Services
SIPRNet	Secret Internet Protocol Router Network
SMD	Service Mediation Descriptions
SOA	Services-Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPAWAR	Space and Naval Warfare Command
SRTM	Security Requirements Traceability Matrix
SSAA	Systems Security Authorization Agreement
SSCC	SPAWAR Systems Center Charleston
SSL	Secure Socket Layer
SWS	Search Web Service
TLR	Tearline Reporting
tModel	Technical Model
TPED	Task, Process, Exploit, Disseminate
TPPU	Task, Post, Process, Use
TTP	Tactics, Techniques, Procedures
TWPDES	Terrorist Watchlist Person Data Exchange Standard
TWS	Trusted Workstation
U-AIM	Ubiquitous Automated Information Manager

UDDI	Universal Description and Discovery Interface
URL	Uniform Resource Locator
USAINSCOM	United States Army Information Security Command
USJFCOM	United States Joint Forces Command
USMTF	United States message text format
USPACOM	United States Pacific Command
USSTRATCOM	United States Strategic Command
V/ID	Visualization/Information Dominance
VEM	Visual Enterprise Monitoring
VKB	Virtual Knowledge Base
VPN	Virtual Private Network
W3C	World Wide Web Consortium – develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential. It is a forum for information, commerce, communication, and collective understanding.
WBS	Work Breakdown Structure
WS	Web Services
WSDL	Web Services Descriptive Language
WSRP	Web Services for Remote Portal
WWW	World Wide Web
XML	Extensible Markup Language

XTCF

